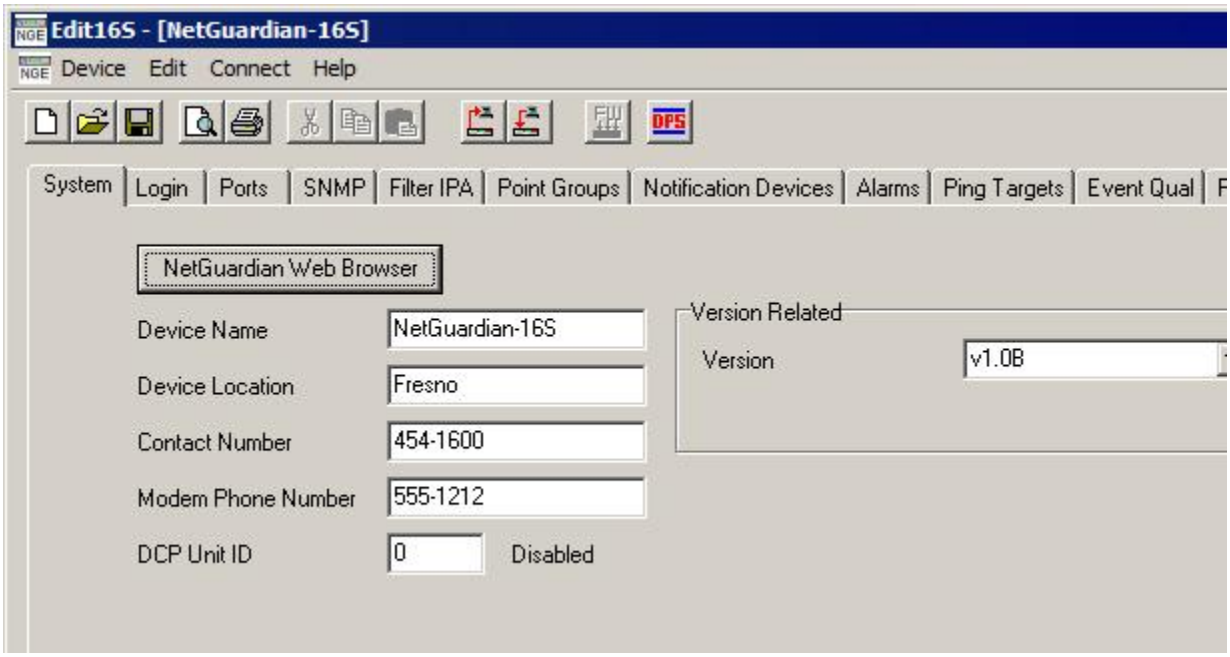
DPS Telecom

"Your Partners In Network Alarm Monitoring"

Edit16S

USER MANUAL



Visit our website at www.dpstelecom.com for the latest PDF manual and FAQs.

December 15, 2006 **D-OC-UM06C.15202** **Software Version 1.0**

Revision History

December 15, 2006	NetGuardian-16S User Manual (D-OC-UM06C.15202) released. Supports Software Version 1.0.
June 30, 2006	NetGuardian-16S User Manual (D-OC-UM066.30300) released. Supports Software Version 1.0.
November 8, 2005	NetGuardian-16S User Manual (D-OC-UM06C.15202) released. Supports Software Version 1.0.

This document contains proprietary information which is protected by copyright. All rights are reserved. No part of this document may be photocopied without prior written consent of DPS Telecom.

All software and manuals are copyrighted by DPS Telecom. Said software and manuals may not be reproduced, copied, transmitted or used to make a derivative work, by either mechanical, electronic or any other means in whole or in part, without prior written consent from DPS Telecom, except as required by United States copyright laws.

© 2006 DPS Telecom

Notice

The material in this manual is for information purposes and is subject to change without notice. DPS Telecom shall not be liable for errors contained herein or consequential damages in connection with the furnishing, performance, or use of this manual.

Contents

Visit our website at www.dpstelecom.com for the latest PDF manual and FAQs

1 Edit16S Overview 1

2 Edit16S PC Requirements 2

3 Connecting to the NetGuardian-16S 2

3.1 ... via Craft Port 2

3.2 ... via LAN 3

4 Getting Started with Edit16S 4

4.1 Edit16S Interface 4

4.2 Edit16S Help 5

4.3 Reading and Writing Configuration Files on PC Disk 5

4.4 Reading and Writing Configuration Files to NetGuardian-16S NVRAM 6

4.5 Importing and Exporting Binary Configuration Files 7

4.6 Printing Configuration File Reports 7

5 System Tab: General Options 8

5.1 Version Related Options 8

5.2 Advanced Settings 9

6 Login Tab: Security Access Options 10

6.1 User Profiles 11

6.2 Access Privileges 11

7 Ports Tab: Configure Network Connections and Data Ports 13

7.1 Ethernet Ports (Private and Public) 13

7.2 Global Ethernet Options 14

7.2.1 Using the Base URL Box 14

7.3 Modem 15

7.4 Craft Port 15

7.4.1 Options Area: Add NetGuardian Expansion Units 16

7.5 Data Ports 17

8 SNMP Tab: SNMP Trap Reporting Options 20

9 Filter IPA Tab: Accept or Block Traffic from Listed IP Addresses 21

10 Point Groups Tab: Organize Alarms in Logical Categories 22

11 Notification Devices Tab: Configure Pager and Email Alarm Notifications 23

11.1 Alphanumeric Pager Setup 26

11.2 Numeric Pager Setup 26

11.3 Text Paging Setup 26

11.4 T/Mon NOC Notification Setup 27

11.5 E-Mail Setup 27

11.5.1 Configuring the NetGuardian-16S's Display Email Address 28

11.5.2 Assigning a Password for SMTP POP3 Authentication 28
11.6 SNMP Paging Setup 29
11.7 TCP Setup 29
11.8 Num17 Pager Setup 30
12 Alarms Tab: Configure Discretes and System Alarms 31
12.1 Configuring Event Qualification Timers 32
12.2 System Alarms 33
13 Ping Targets Tab: Configure Ping Alarms 34
14 Event Qual Tab: View All Event Qualification Times 35
15 Relays Tab: Configure Control Relays 36
16 Timers Tab: Configure Ping Cycles, Timeouts and Refresh Rates 37
16.1 Timer Descriptions 37
17 Time Settings Tab 39
18 Call List Tab: Configure Voice Call Out 39
18.1 Global Voice Call Out Settings 39
18.2 Contact-Specific Voice Call Out Settings 40
18.3 Voice Call Out Sequence of Operations 41
19 Voice Call Out Default Dialogs 42
19.1 Dialog 1: Default Critical 42
19.2 Dialog 2: Default Major 42
19.3 Dialog 3: Default Secure Dial-In 43
19.4 Dialog 4: Critical GR-474 43
19.5 Dialog 5: Major GR-474 44
19.6 Dialog 6: GR-474 Secure Dial-In 44
19.7 Dialog 7: Critical RUS-FORM-522 45
19.8 Dialog 8: Major RUS-FORM-522 45
19.9 Dialog 9: RUS-FORM-522 Secure Dial-In 46
20 Firmware Load 47
20.1 Loading Firmware on a Single NetGuardian-16S Unit 48
20.2 Loading Firmware to Multiple NetGuardian-16S Units Using Saved Configuration Files (The Easy Way) 49
20.3 Loading Firmware to Multiple NetGuardian-16S Units Using a Script File 50
21 Reference Section 52
21.1 NetGuardian-16S Alarm Map 52
21.2 System Alarm Descriptions 53
21.3 NetGuardian-16S Trap OIDs 54
21.4 SNMP Granular Trap Packets 55
22 Technical Support 56

1 Edit16S Overview

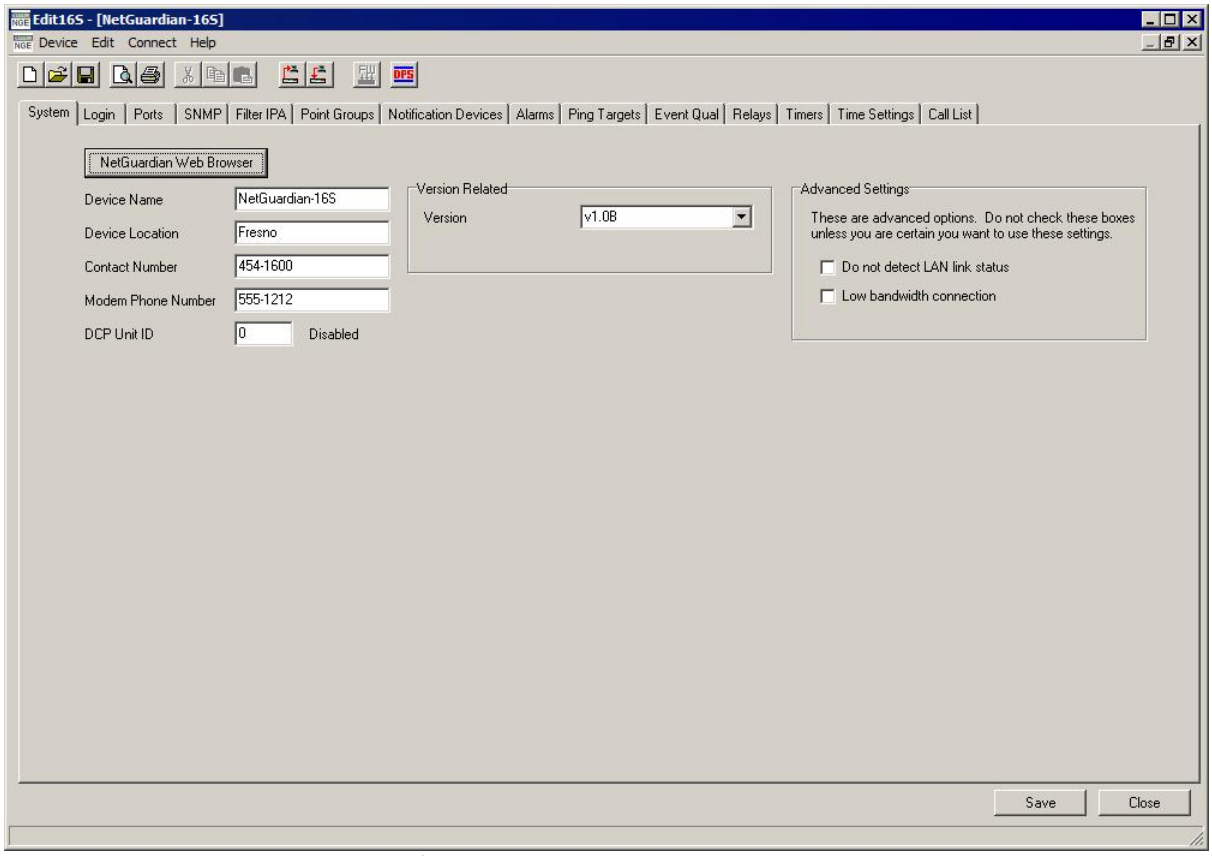


Fig 1.1. *The Edit16S user interface*

Edit16S is the System Administrator's configuration interface for the NetGuardian-16S. Edit16S gives you full control over all of the NetGuardian-16S's configurable options, unlike the limited configuration options available in the NetGuardian-16S's built-in Web Browser Interface.

With Edit16S, you can:

- Configure and provision the NetGuardian-16S.
- Read and write configuration files to NetGuardian-16S units in the field over LAN or local craft port connection.
- Create and save configuration files to your local PC — this is great if you want to create a standard configuration for all your NetGuardian-16S units, or if you want to create batches of configuration files for remote LAN upload.
- Load firmware updates via LAN.

To install Edit16S on your PC, run the installer program included on the NetGuardian-16S Resource CD.

2 Edit16S PC Requirements

To run Edit16S, DPS Telecom recommends a Windows-based PC with the following specifications:

Operating System: Windows 9x, NT, ME, 2000 or XP

Processor: 333 MHz or better

Color Setting: 16 bit

Screen Resolution: 1024 x 768

Note: Edit16S may not work properly on slower machines if the display is set for 256 colors.

3 Connecting to the NetGuardian-16S

3.1 ... via Craft Port

Fig. 3.1.1. *To use Edit16S over a craft port connection, use the* ***UPPER*** *craft port*

The simplest way to connect to the NetGuardian-16S is over a physical cable connection between your PC's COM port (always COM Port 1) and the NetGuardian-16S's **UPPER** craft port. **Note:** You don't have to be connected a NetGuardian-16S unit to use Edit16S. You only need a connection to the unit to read or write configuration files to its NVRAM. You can use Edit16S on an unconnected PC to create and store NetGuardian-16S configuration files.

Use the DB9M-DB9F download cable provided with your NetGuardian-16S to make a craft port connection. Edit16S can only connect to the NetGuardian-16S through the **upper** craft port, **not the lower craft port**. Each craft port is connected to a different circuit board, and you need to connect to the upper circuit board. For more details on the craft ports, including their pinout, see the NetGuardian-16S User Manual.

You can perform all configuration tasks via the craft port — but if you like, you can connect via the craft port just to configure the NetGuardian-16S's Private LAN IP address, and then do the rest of your configuration via a LAN connection.

For details on initiating a connection to the NetGuardian-16S, see Section 4.4, "Reading and Writing Configuration Files to NetGuardian-16S NVRAM."

3.2 ... via LAN

Fig. 3.2.1. *NetGuardian-16S LAN ports*

You can also connect to the NetGuardian-16S over a LAN connection. This is a very convenient way to provision multiple NetGuardian-16S units at multiple locations. **Note:** You don't have to be connected a NetGuardian-16S unit to use Edit16S. You only need a connection to the unit to read or write configuration files to its NVRAM. You can use Edit16S on an unconnected PC to create and store NetGuardian-16S configuration files.

The NetGuardian-16S has two Ethernet ports: the Private port, which connects to the company LAN; and the Public port, which connects to the public Internet. Each port has a separate IP address. (For details about the Ethernet ports, including their pinout, see the NetGuardian-16S User Manual.)

To connect to the NetGuardian-16S via LAN, all you need is the unit's Private or Private IP address. If the unit has not yet been assigned an IP address, you must make a temporary connection the unit to configure its IP settings.

If you have physical access to the NetGuardian-16, the easiest thing to do is connect to the unit through the craft port and then assign it an IP address. Then you can complete the rest of the unit configuration over a remote LAN connection, if you want. For instructions, see:

- Section 3.1 "Connecting to the NetGuardian-16S via Craft Port."
- Section 7, "Ports Tab: Configure Network Connections and Data Ports."
- Section 4.4, "Reading and Writing Configuration Files to NetGuardian-16S NVRAM."

If you DON'T have physical access to the NetGuardian-16, you can make a LAN connection to the unit by temporarily changing your PC's IP address and subnet mask to match the NetGuardian-16S's factory default IP settings. Follow these steps:

1. Look up your PC's current IP address and subnet mask, and write this information down.
2. Reset your PC's IP address to **192.168.1.200**.
3. Reset your PC's subnet mask to **255.255.0.0**. You may have to reboot your PC to apply your changes.
4. Start Edit16S.
5. On the **Ports** tab, enter the assigned Private or Private IP address for this NetGuardian-16S unit. For detailed instructions, see Section 7, "Ports Tab: Configure Network Connections and Data Ports."
6. Write the new IP settings to the NetGuardian-16S's NVRAM. For detailed instructions, see Section 4.4 "Reading and Writing Configuration Files to NetGuardian-16S NVRAM."
7. Reset your PC's original IP address and subnet mask.
8. You can now connect to the NetGuardian-16S over its new assigned IP address.

4 Getting Started with Edit16S

4.1 Edit16S Interface

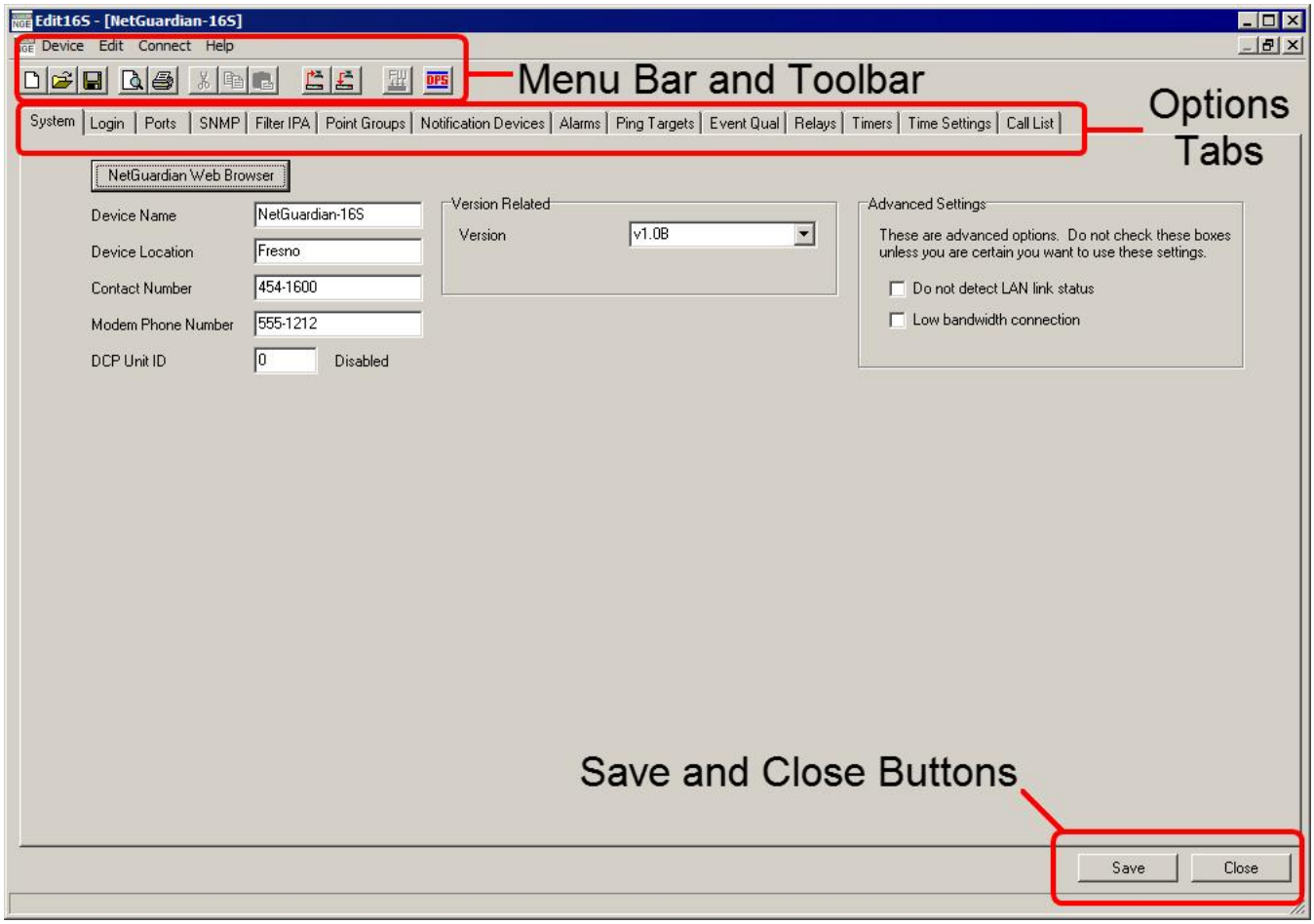


Fig. 4.1.1 *The Edit16S interface*

Edit16S provides a standard Windows interface for selecting configuration options and working with configuration files.

The **menu bar** and **toolbar** contain commands for opening and saving configuration files on PC disks and reading and writing configurations to the NetGuardian-16S's NVRAM.

Each **options tab** contains configuration settings for a specific NetGuardian-16S function. Each configuration tab is defined in detail in this manual.

At the bottom right of the Edit16S window are **Save** and **Close** buttons (you may have to scroll or grow the window to see them). The **Save** button saves your configuration file to PC disk (providing the same function as the **Save Device** command in the **File** menu and toolbar). The **Close** button closes the current Edit16S configuration file.

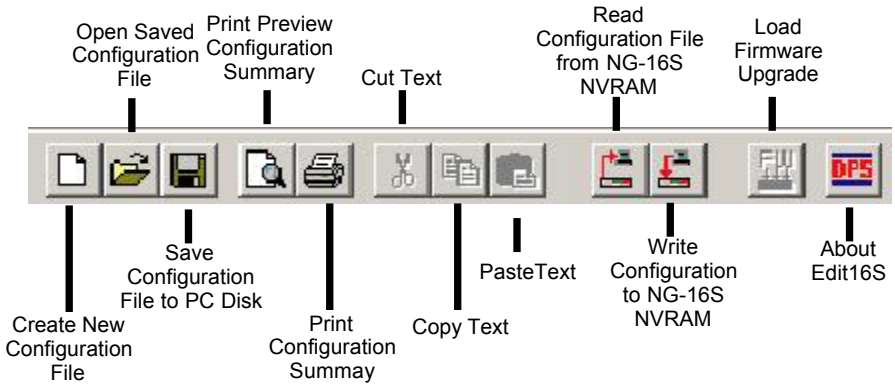


Fig. 4.1.2. *Edit16S toolbar*

The **toolbar** provides convenient access to some of Edit16S's most frequently used commands. When you point your mouse cursor at a toolbar button, text explaining the button's function will appear in the Status Bar at the bottom of the Edit16S window.

Some menu and toolbar commands are grayed out and unavailable when you first start Edit16S. These commands are only available when a configuration file is open. To make all Edit16S commands available, create a new configuration file, open a saved configuration file from disk, or read a configuration file from the NetGuardian-16S's NVRAM.

4.2 Edit16S Help

To read the help file, choose **Help** from the **Help** menu. To see an explanation of the function of a toolbar button or text box, point your mouse cursor at the button or text box, and some brief explanation text will appear in the status bar at the bottom of the Edit16S window. Some options tabs contain explanatory text explaining your options.

4.3 Reading and Writing Configuration Files on PC Disk

NetGuardian-16S configurations can be saved to and loaded from a floppy or PC hard disk or network drive. Working with saved configuration files is a very convenient way to configure multiple NetGuardian-16S units — you can define a basic configuration for all your units, save it on disk, and use it (with appropriate changes) for all of your individual units.

Commands for working with configuration files on your PC are located on the left side of the toolbar (see Figure 4.1.2). The available commands are:

New: Create a new, blank configuration. (**Note:** This will clear all Edit16S configuration settings; you will be prompted to save the current configuration.)

Open: Load an existing saved configuration file from disk.

Save: Save current configuration.

To delete a NetGuardian-16S configuration file from your PC, choose **Delete Device** from the **Device** menu. A dialog box will open to show you the configuration files on your computer. Select the file you want to erase and click **Delete**. A confirmation prompt will appear. Click **Yes** to continue the deletion or **No** to cancel. **Deletion cannot be reversed, so be sure you want to delete the file**.

4.4 Reading and Writing Configuration Files to NetGuardian-16S NVRAM

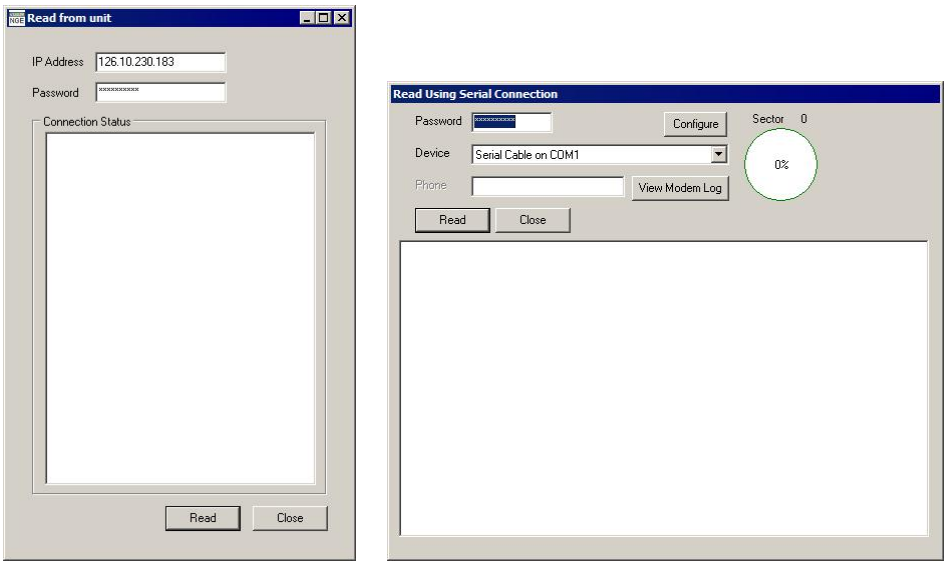


Fig. 4.4.1. *Read from unit via LAN (left) or via craft port (right)*

Edit16S's main function is to write configuration files to the NetGuardian-16S's NVRAM. You can also load configurations from a unit's NVRAM, edit them as you please, and then rewrite them to NVRAM.

To read from NVRAM, click the **Read NVRAM** button on the toolbar or choose **Read from NetGuardian** from the **Connect** menu. (If you choose the command from the **Connect** menu, you also get to choose whether you connect to the NetGuardian-16S via craft port or LAN.)

One of the two dialogs shown in Figure 4.4.1 will open. You **must** have the correct password to read the NVRAM. If connecting by LAN, enter the NetGuardian-16S's **Private** or **Public** IP address. Click the **Read** button. The dialog will display the progress of the reading process. When the read is complete, the dialog box will close and the configuration file will be open in Edit16S.

Note: Reading from the NetGuardian-16S's NVRAM will clear all configuration settings currently defined in the Edit16S window.

It's a good idea to always load the existing configuration from unit NVRAM **before** defining configuration options. This is an important double check to make sure you know what unit you're working with and what settings you're changing.

To write to NVRAM, click the **Write NVRAM** button on the toolbar or choose **Write to NetGuardian** from the **Connect** menu. (If you choose the command from the **Connect** menu, you also get to choose whether you connect to the NetGuardian-16S via craft port or LAN.)

A dialog box similar to those shown in Figure 4.4.1 will open You **must** have the correct password to read the NVRAM. If connecting by LAN, enter the NetGuardian-16S's **Private** or **Public** IP address. Click the **Write** button. The dialog will display the progress of the writing process. When the write is complete, the dialog box will close and Edit16S will automatically reboot the NetGuardian-16S.

Note: Changes to the NetGuardian-16S configuration **DO NOT** take effect until you write the changes to NVRAM and reboot the unit. The **Write NVRAM** command writes **all current configuration settings** to the NetGuardian-16S's NVRAM, **erasing all previous settings**.

4.5 Importing and Exporting Binary Configuration Files

Fig. 4.5.1. *Import from File and Export to File commands*

You can also transfer binary format NetGuardian-16S files directly from NVRAM to your PC using File Transfer Protocol. These files can be imported to Edit16S using the **Import from File** command on the **Device** menu. (See Figure 4.5.1, above.).

Similarly, NetGuardian-16S configurations created or editing using Edit16S can be exported in binary format using the **Export to File** command on the **Device** menu. The binary format configuration file can then be transferred to the NetGuardian-16S's NVRAM using FTP. (You must reboot the NetGuardian-16S for the new configuration to take effect.)

4.6 Printing Configuration File Reports

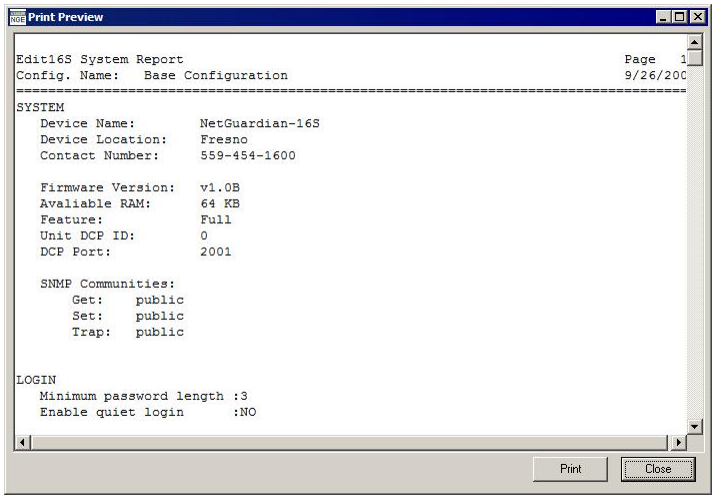


Fig. 4.6.1. *Print preview of configuration report*

NetGuardian-16S configuration settings can be printed out for easy reference, using either the **Print** command on the **Device** menu or the **Print** button on the toolbar. To preview what the configuration printout will look like, choose the **Print Preview** command from either the **Device** menu or the toolbar. The **Print Preview** command opens a scrolling text window, as shown in Figure 4.6.1, above.

5 System Tab: General Options

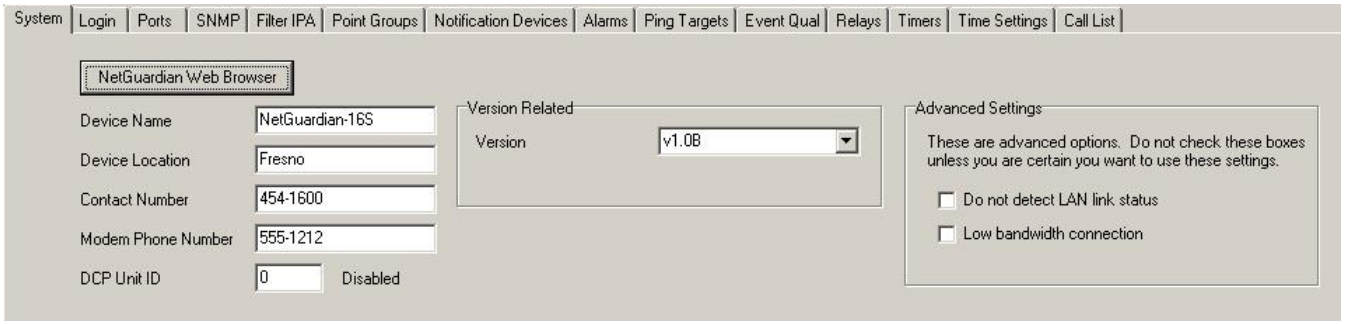


Fig. 5.1. *System tab*

The **System** tab (Figure 5.1) provides options for configuring basic NetGuardian-16S setup:

Device Name: Assign the NetGuardian-16S a name of your choice. For easy identification, it's a good idea to assign a name that will be meaningful to everyone who uses the NetGuardian-16S.

Device Location: Type in the physical location of the NetGuardian-16S. This is very useful for keeping track of different units.

Note: The **Device Name** and **Device Location** boxes are also used to assign the NetGuardian-16S a display email address used in email alarm notifications. For details, see Section 11.5.1, "Configuring the NetGuardian-16S's Display Email Address."

Contact Number: Type in a phone number or email address for the person responsible for this NetGuardian-16S unit.

Modem Phone Number: Type in the phone number assigned to the NetGuardian-16S's internal modem.

DCP Unit ID: Type in the DCP address identifying this NetGuardian-16S to T/Mon NOC. (If set to 0, DCP reporting to T/Mon NOC will be disabled and the word "Disabled" will appear just beneath and to the right of the **DCP Unit ID** box, as shown in Figure 5.1, above.)

The **NetGuardian Web Browser** button opens a Web Browser Interface connection to the NetGuardian-16S unit, if the unit has been configured with a valid IP address.

5.1 Version Related Options

The **Version Related** area displays the firmware version loaded on the NetGuardian-16S unit. Your NetGuardian-16S shipped with the most recent available firmware, but firmware updates will be released from time to time. After installing a firmware update, you can use the **Version** drop-down menu to select the newer firmware version to access new features.

5.2 Advanced Settings

The **Advanced Settings** area displays some check boxes for two options that should only be checked if you are certain you want to use them:

Do not detect LAN link status: Check this option if your NetGuardian-16S will normally operate without any LAN connection. This option will stop monitoring of the LAN link and prevent the audible Ethernet Connection Failure alarm from sounding.

Low bandwidth connection: Check this option if you have a low-bandwidth connection to the NetGuardian-16S.

Note: In v1.0F, the following option is also available:

Disable all audible (Not Recommended): Check this option to disable audible notification from the NetGuardian-16S speaker. (**Warning:** Disabling the speaker is not recommended and could be dangerous.)

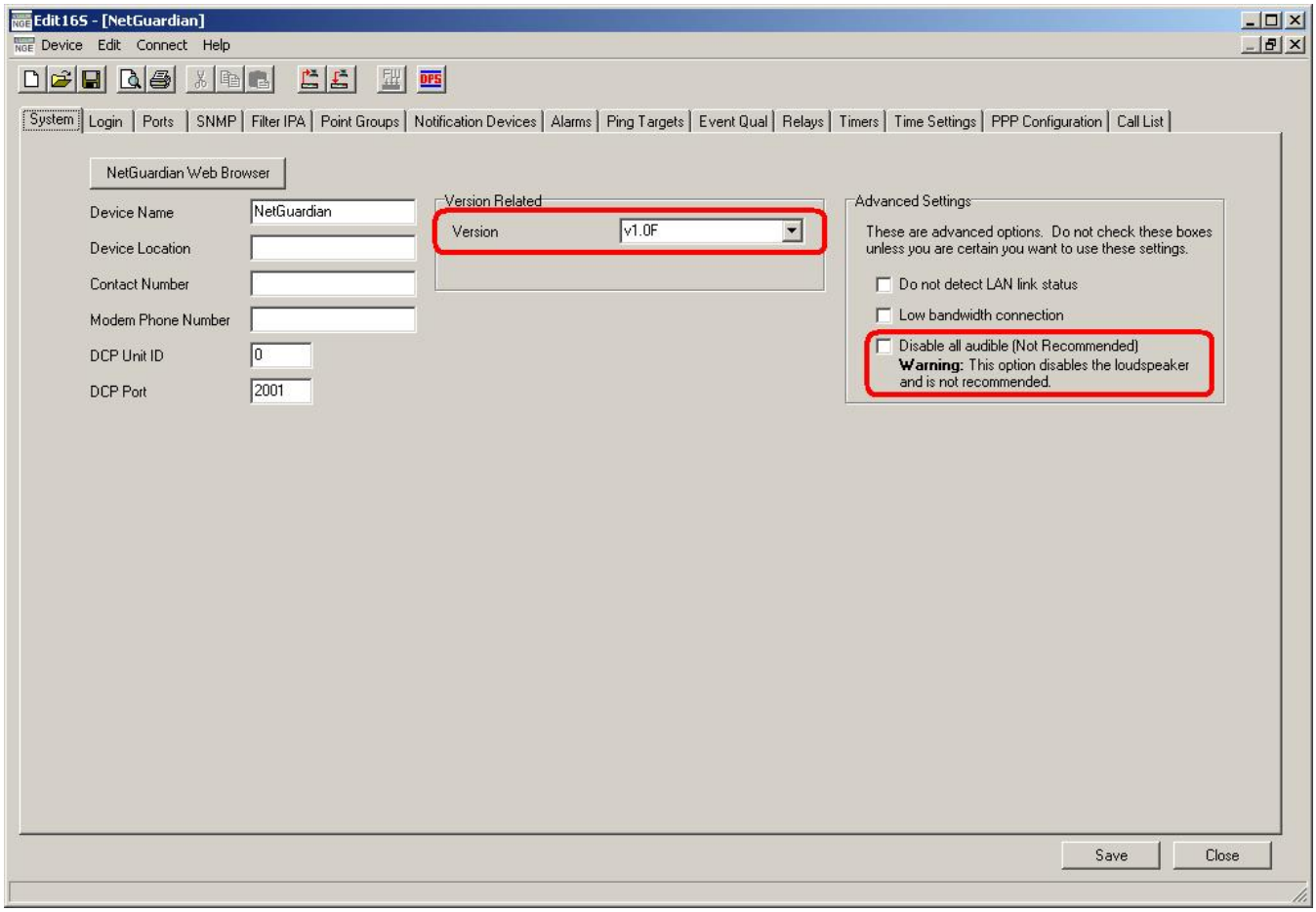

Edit16S - [NetGuardian]
Device Edit Connect Help
System Login Ports SNMP Filter IPA Point Groups Notification Devices Alarms Ping Targets Event Qual Relays Timers Time Settings PPP Configuration Call List
NetGuardian Web Browser
Device Name
NetGuardian
Device Location
Contact Number
Modem Phone Number
DCP Unit ID
0
DCP Port
2001
Version Related
Version
v1.0F
Advanced Settings
These are advanced options. Do not check these boxes unless you are certain you want to use these settings.
Do not detect LAN link status
Low bandwidth connection
Disable all audible (Not Recommended)
Warning: This option disables the loudspeaker and is not recommended.
Save
Close

Fig. 5.2- *The Disable All Audible option in v1.0F*

6 Login Tab: Security Access Options

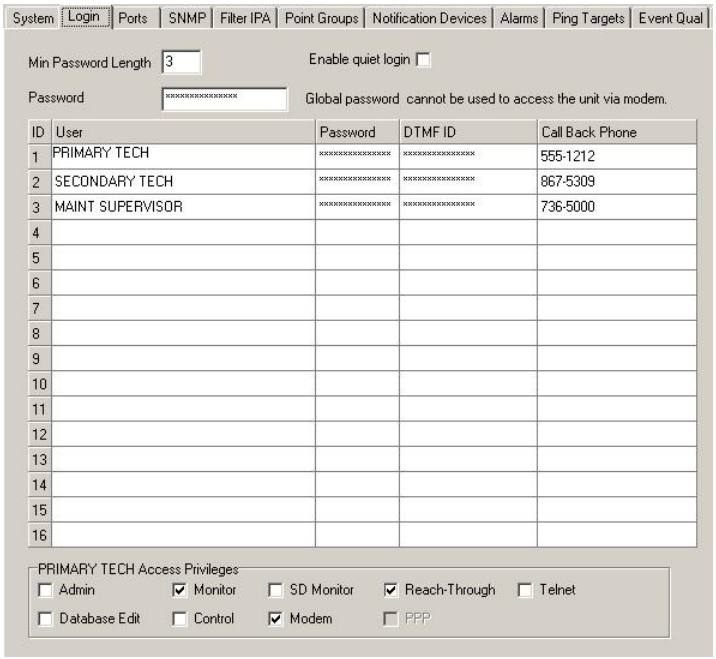


Fig. 6.1. *Login tab*

The **Login** tab (Figure 6.1) provides options for configuring NetGuardian-16S users and their security access privileges. Clicking on the **Login** tab first opens a security dialog box that will prompt you to enter the **Master** password — the password that allows complete access to configure all NetGuardian-16S options. The factory default Master password for a new NetGuardian-16S or new Edit16S configuration file is `dpstelecom` — note that `dpstelecom` is all lower-case; passwords are case sensitive. For better security, you should change the default Master password immediately.

After you have provided the Master password, you have access to the following options:

Min Password Length: Minimum number of characters for any user password. The longer your passwords are, the more difficult they are to guess.

Fig. 6.2. *Changing the Master password*

Password: This box displays the current Master password in asterisks. To change the Master password, start typing in this box. The **Master Password** dialog box (Figure 6.2, above) will open (your typing will automatically appear in the **Password** box in this window). Enter the new password again to confirm, then click **OK**.

Enable quiet login: Checking this box hides password asterisks for users logging in via modem, which provides extra security for their passwords.

6.1 User Profiles

You can enter up to 16 **User Profiles**, each with its own security access privileges. The User Profile options are:

User: Type in a name or description for each user. This box has an 18 character limit.

Fig. 6.1.1. *Assigning a user password*

Password: Type in a password for the user. A dialog box like that shown in Figure 6.1.1 (above) will open (your typing will automatically appear in the **Password** box in this window). Enter the new password again to confirm, then click **OK.**

Call Back Phone: This is a security feature that prevents unauthorized access via modem. When dial-up users connect to the NetGuardian-16S, they are prompted to enter their passwords. If the user's password is valid, the NetGuardian-16S will display the message `accepted, Disconnecting`. The NetGuardian-16S then disconnects and dials the user's modem, and the user will be logged on with his or her defined access privileges. To disable this feature, leave the **Call Back Phone** box blank.

6.2 Access Privileges

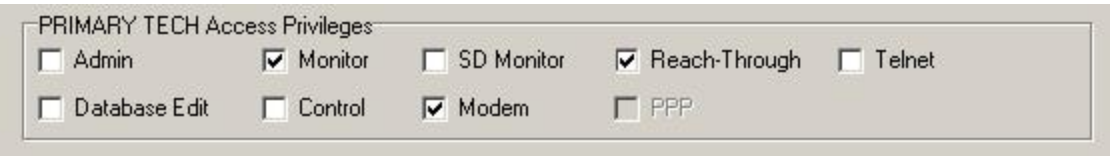


Fig. 6.2.1. *Configuring access privileges*

The **Access Privileges** area provides check boxes for configuring each user's security access rights. The display changes to show the Access Privileges for the user currently selected in the User Profiles area. For each user, the Access Privilege levels are:

Admin: Allows user to change Login User Profiles and passwords

Database Edit: Allows user to edit the NetGuardian-16S configuration database

Monitor: Allows the user to monitor NetGuardian-16S alarm points

Control:	Allows user to operate NetGuardian-16S control relays
SD Monitor:	Allows user to monitor serial port traffic
Modem:	Allows user to access NetGuardian-16 via dial-up modem connection
Reach-Through:	Allows user proxy access through reach-through data ports
Telnet:	Allows user Telnet and craft access to NetGuardian-16S

7 Ports Tab: Configure Network Connections and Data Ports

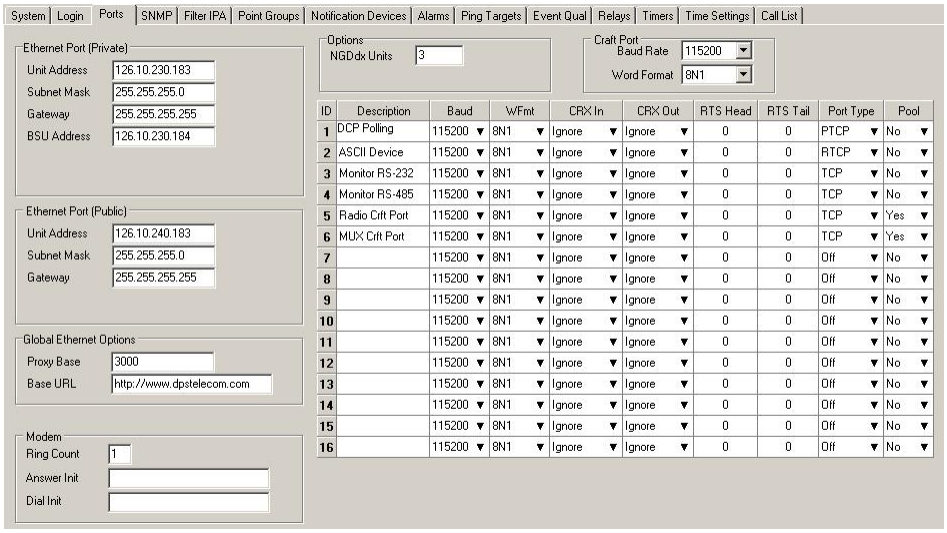

System
Login
Ports
SNMP
Filter IPA
Point Groups
Notification Devices
Alarms
Ping Targets
Event Qual
Relays
Timers
Time Settings
Call List
Ethernet Port (Private)
Unit Address 126.10.230.183
Subnet Mask 255.255.255.0
Gateway 255.255.255.255
BSU Address 126.10.230.184
Ethernet Port (Public)
Unit Address 126.10.240.183
Subnet Mask 255.255.255.0
Gateway 255.255.255.255
Global Ethernet Options
Proxy Base 3000
Base URL http://www.dpstelecom.com
Modem
Ring Count 1
Answer Init
Dial Init
Options
NGDdx Units 3
Craft Port
Baud Rate 115200
Word Format 8N1
ID Description Baud WFmt CRX In CRX Out RTS Head RTS Tail Port Type Pool
1 DCP Polling 115200 8N1 Ignore Ignore 0 0 PTCP No
2 ASCII Device 115200 8N1 Ignore Ignore 0 0 RTCP No
3 Monitor RS-232 115200 8N1 Ignore Ignore 0 0 TCP No
4 Monitor RS-485 115200 8N1 Ignore Ignore 0 0 TCP No
5 Radio Crft Port 115200 8N1 Ignore Ignore 0 0 TCP Yes
6 MUX Crft Port 115200 8N1 Ignore Ignore 0 0 TCP Yes
7 115200 8N1 Ignore Ignore 0 0 Off No
8 115200 8N1 Ignore Ignore 0 0 Off No
9 115200 8N1 Ignore Ignore 0 0 Off No
10 115200 8N1 Ignore Ignore 0 0 Off No
11 115200 8N1 Ignore Ignore 0 0 Off No
12 115200 8N1 Ignore Ignore 0 0 Off No
13 115200 8N1 Ignore Ignore 0 0 Off No
14 115200 8N1 Ignore Ignore 0 0 Off No
15 115200 8N1 Ignore Ignore 0 0 Off No
16 115200 8N1 Ignore Ignore 0 0 Off No

Fig. 7.1. *Ports tab*

The **Ports** tab (Figure 7.1) provides options for configuring the NetGuardian-16S's Ethernet ports, modem, craft port and data ports.

7.1 Ethernet Ports (Private and Public)

The NetGuardian-16S has two Ethernet ports, the **Private** port and the **Public** port. Each port has its own separate IP address and subnet, so you can safely connect one port to your private company LAN and the other to the public Internet.

Each of the NetGuardian-16S's Ethernet ports has its own configuration area on the **Ports** tab. For each Ethernet port, your options are:

Unit Address: Type in the IP address assigned to this port. (Note that the Private and Public ports must have separate IP addresses on separate subnets.)

Subnet Mask: Type in the subnet mask assigned to this port. (The subnet mask controls whether IP packets transmitted to and from the NetGuardian-16S stay within the local network or are forwarded somewhere else on a wide area network.

Gateway: You only need to enter a default gateway if this port is connected to a wide area network. If you're not connected to a WAN, keep the default value, **255.255.255.255**.

Private Port Only Option
The following options is available only for the Private port:

BSU Address: Type in the IP address of the CopperCom CopperController. This is the IP address the NetGuardian-16S will perpetually ping to verify its connection to the CopperController. If the CopperController does not respond to the ping, the NetGuardian-16S will enter Standalone Mode. (For details on Standalone Mode, see the NetGuardian-16S User Manual.)

7.2 Global Ethernet Options

The **Global Ethernet Options** area provides two options that apply to both Ethernet ports:

Proxy Base: Defines the TCP/IP ports used by Data Ports 1–16. Data Port 1 receives the port number entered in the **Proxy Base** box, and Data Ports 2–16 receive the next 15 port numbers in ascending order. For example, if you keep the default setting of 3000, Data Ports 1–16 will correspond to TCP/IP ports 3000–3015.

Base URL: This is an optional box that you should only fill in if you want alarm points in the Web Browser Interface to be clickable hyperlinks to Web pages or other browser-viewable files. To use this option, type in the URL of the website that hosts your Web files. For complete instructions on using this feature, see Section 7.2.1, "Using the Base URL Box."

7.2.1 Using the Base URL Box

Entering a URL in the **Base URL** box on the **Ports** tab enables a feature that adds clickable hyperlinks to each alarm point in the NetGuardian-16S Web Browser Interface. These hyperlinks can take the user to HTML Web pages or any other file that can be viewed in a Web browser, like Microsoft Word documents, PDF files, text files, and so on.

You can use this feature to provide users with quick access to explanations of the alarm, specific instructions for handling the alarm, equipment documentation, or any other information you think is relevant to the alarm.

To use this feature, you must first create a website to host the pages or files you want to link to. Then enter the website's URL in the **Base URL** box on the **Ports** tab. This automatically activates hyperlinks in the Web Browser Interface.

Web Browser Interface Page	Linked Web Page File Names
Base Alarms	base1.html–base32.html
Ping Alarms	ping1.html–ping32.html
System Alarms	system9.html–system16.html; system33.html–system50.html

Table 7.2.1.A. *File name formats for linked Web pages*

The pages you create for the Web Browser Interface must have specific file names. The basic format for Web page file names is shown in Table 7.2.1.A, above. Some examples: If your website's URL is http://www.mycompany.com, the Web page for Base Alarm Point 5 should be http://www.mycompany.com/base5.html, the Web Page for Ping Alarm Point 28 should be http://www.mycompany.com/ping28.html, and so on.

To link to files other than HTML pages, include the text **/&pntID;** plus a file extension to your base URL. For example, to link to PDF documents, type in your base URL like this: http://www.mycompany.com/&pntID;.pdf. To link to a Microsoft Word document, type in your base URL like this: http://www.mycompany.com/&pntID;.doc.

7.3 Modem

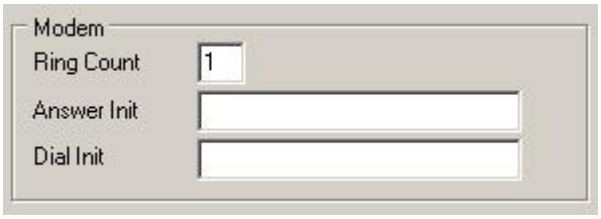


Fig. 7.3.1. *Modem configuration*

The **Modem** area configures basic settings for the internal modem:

Ring Count: Number of rings before the modem answers incoming calls. Default setting is 1.

Answer Init and **Dial Init:** Type in these boxes only if any other modem initialization settings need to be set. For example, the modem can be set to ignore the dial tone by entering an init string in either of these boxes. Refer to the standard Hayes modem command set for a list of modem commands. The default setting for these boxes is blank.

7.4 Craft Port

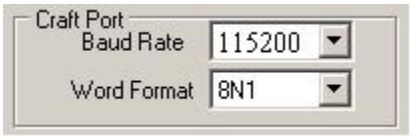


Fig. 7.5.1. *Craft port configuration*

The **Craft Port** area provides the following options for configuring the NetGuardian-16S craft port:

Baud Rate: Choose from 1200, 2400, 9600, 19200, 38400, 57000 or 115200 baud. Default setting is 115200.

Word Format: Choose from 8N1, 7E1, or 701. Default setting is 8N1.

7.4.1 Options Area: Add NetGuardian Expansion Units

Fig. 7.4.1. *Options area*

The **Options** area on the **Ports** tab provides only one option: the **NGDdx Units** box, which provisions the NetGuardian-16S with the number of connected NetGuardian Expansion units. The only configuration necessary is to type in the number of NetGuardian Expansion Units, from 0–3.

Up to three NetGuardian Expansion units can be daisy-chained from the NetGuardian-16S. Each NetGuardian Expansion unit adds 48 discrete alarm points and, optionally, 8 control relays to the NetGuardian-16S's alarm capacity, for configurations of:

- 1 NetGuardian Expansion unit: 80 discrete alarms and (option) 16 control relays
- 2 NetGuardian Expansion units: 128 discrete alarms and (option) 24 control relays
- 3 NetGuardian Expansion units: 176 discrete alarms and (option) 32 control relays

To order NetGuardian Expansion units, call DPS Telecom at **1-800-622-3314**.

7.5 Data Ports

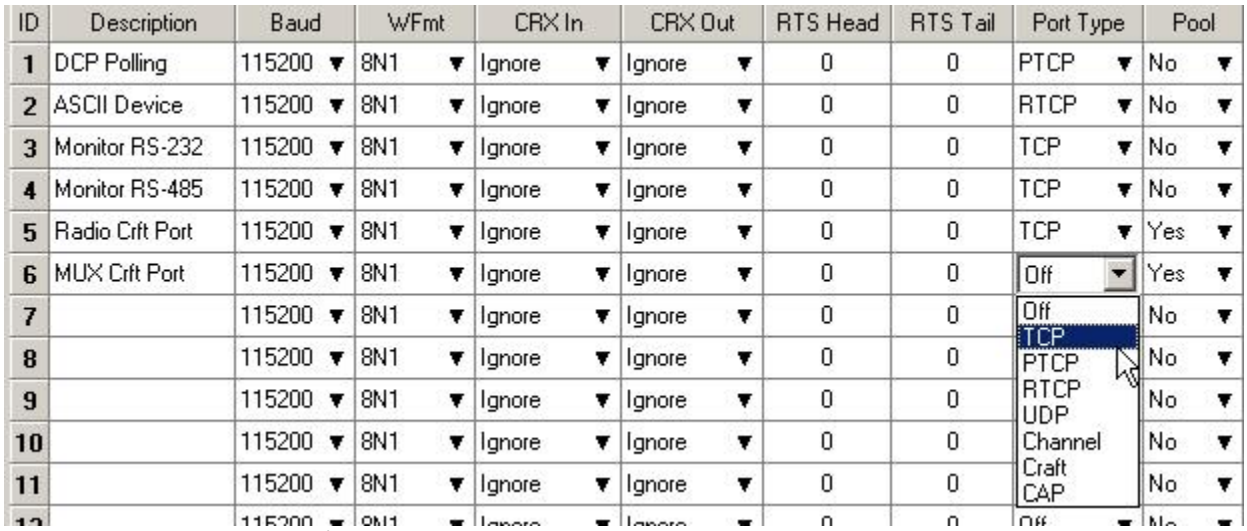

ID
Description
Baud
WFmt
CRX In
CRX Out
RTS Head
RTS Tail
Port Type
Pool
1 DCP Polling 115200 8N1 Ignore Ignore 0 0 PTCP No
2 ASCII Device 115200 8N1 Ignore Ignore 0 0 RTCP No
3 Monitor RS-232 115200 8N1 Ignore Ignore 0 0 TCP No
4 Monitor RS-485 115200 8N1 Ignore Ignore 0 0 TCP No
5 Radio Crft Port 115200 8N1 Ignore Ignore 0 0 TCP Yes
6 MUX Crft Port 115200 8N1 Ignore Ignore 0 0 Off Yes
7 115200 8N1 Ignore Ignore 0 0 No
8 115200 8N1 Ignore Ignore 0 0 No
9 115200 8N1 Ignore Ignore 0 0 No
10 115200 8N1 Ignore Ignore 0 0 No
11 115200 8N1 Ignore Ignore 0 0 No
Off
TCP
PTCP
RTCP
UDP
Channel
Craft
CAP

Fig. 7.5.1. *A portion of the Data Ports definition table*

The **Data Ports** definition table configures options for the NetGuardian-16S's 16 data ports. Please note that the NetGuardian Expansion unit is connected to the NetGuardian-16S using the dedicated NetGuardian Expansion port. This port requires no user configuration. (For more information on the NetGuardian Expansion port, see the NetGuardian-16S User Manual.)

For each data port, your choices are:

Description: Type in a description of the function or device connected to the data port. This box has a 15 character limit.

Baud: Choose from 1200, 2400, 9600, 19200, 38400, 57000 or 115200 baud. Default setting is 115200.

WFmt: Word format. Choose from 8N2, 8N1, 7N1, 7E1, 8O2 or 701. Default setting is 8N1.

CRX In: Carriage Return In. This function is used to customize carriage returns (Hex 0D) at the ends of line feeds (Hex 0A). Choose 'Append' to add a carriage return to all incoming line feeds. "Remove" to remove a return, or "Ignore" to accept all carriage returns as received. Default setting is Ignore. This setting allows you to troubleshoot formatting issues.

CRX Out: Carriage Return Out. This function is used to customize carriage returns (Hex0D) at the ends of line feeds (Hex 0A). Choose 'Append' to add a carriage return to all outgoing line feeds. "Remove" to remove a return, or "Ignore" to add no returns. Default setting is Ignore. This setting allows you to troubleshoot formatting issues.

RTS Head: Request To Send. Time carrier is turned on before data is sent, in milliseconds. Available range is 0–255 milliseconds.

RTS Tail: Request To Send. Time carrier stays on after data is sent, in milliseconds. Available range is 0–255 milliseconds.

Port Type: Each data port can be configured for several different port types. TCP is the default port type. For an explanation of the port type options, see Table 7.4.A, below.

Pool: Choose **Yes** from the **Pool** drop-down menu to pool data ports together. To use port pooling, at least two data ports must be assigned to the pool. When port pooling is activated, if you telnet directly to any port in the pool and the port is busy, the NetGuardian-16S will automatically connect you to another port from the pool if one is available. Port pooling can only be used with TCP, RTCP and PTCP ports.

Note: There are no echo settings for the data ports.The data ports are pre-set to no echo.

Port Type	Description
TCP	Reach-through port via Telnet over TCP/IP.
PTCP	Permanent TCP. During a proxy connection, this connection will never time out. PTCP is **not recommended** for the NetGuardian-16S
RTCP	Raw TCP with no Telnet negotiation.
UDP	Reach-through port via Telnet over UDP/IP (reserved for future use).
Channel	Creates logical bridge to odd/even partner. The odd/even partners are pairs of 1-2, 3-4, 5-6, and 7-8. This allows the NetGuardian-16S to view communication traffic in either direction when inserted in the serial communication path between two devices. This is accomplished by going “in” to the NetGuardian with one device and “out” to the other device from the odd/even partner port. Data is passed directly from one port to its odd/even partner without being altered in any way. This ability greatly simplifies troubleshooting communication problems by isolating the non-communicating device. When CHAN is selected, the NetGuardian automatically activates the odd/even partner as CHAN.
Craft	Data port acts as a craft port.
CAP	Captures debug information from connected device. The debug information is stored in the receive queue of the NetGuardian-16S. This is used primarily as a troubleshooting feature.

Table 7.4.A. *Port type options*

8 SNMP Tab: SNMP Trap Reporting Options

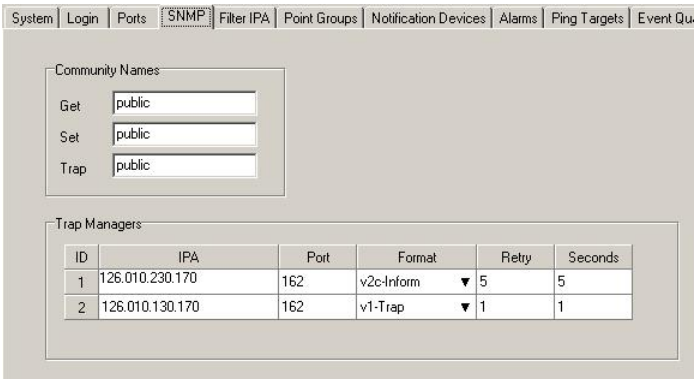


Fig. 8.1. *SNMP tab*

The **SNMP** tab (Figure 8.1) provides the following options for configuring SNMP Trap reporting:

SNMP Communities

Get: Community string for SNMP Get requests.

Set: Community string for SNMP Set requests.

Trap: Community string for SNMP Traps.

Note: Make sure that your community strings match those used by the SNMP manager. Community strings are security passwords; if the strings do not match, the SNMP manager will not accept Traps from the NetGuardian-16S. Community strings are case sensitive.

Trap Managers

The NetGuardian-16S can report alarms as SNMP Traps to two separate SNMP managers at different IP addresses. For each SNMP manager you can configure the following options:

IPA: IP address of the SNMP manager If you're configuring the NetGuardian-16S to report to only one SNMP manager, keep the default setting (255.255.255.255) in the IPA filed of Trap Manager ID 2. To turn off SNMP Trap reporting completely, keep the default setting for both Trap Manager IDs.

Trap Port: UDP/IP port the SNMP manager uses to receive Traps. In most cases, you should keep the default setting, which is 162.

Format: Choose between SNMP v1-Trap, SNMP v2c-Trap, or SNMP v2c-Inform. (An SNMP v2c Inform message provides confirmed delivery, unlike a Trap message. When an SNMP manager receives an Inform, it sends a confirmation response back to the SNMP agent device that sent the Inform. If the SNMP agent device doesn't receive a response to its Inform, it resends the Inform until the SNMP manager sends a confirmation response.)

Retry: Number of times the NetGuardian-16S will resend SNMP v2c Informs.

Seconds: Time interval in seconds between attempts to resend SNMP v2c Informs.

9 Filter IPA Tab: Accept or Block Traffic from Listed IP Addresses

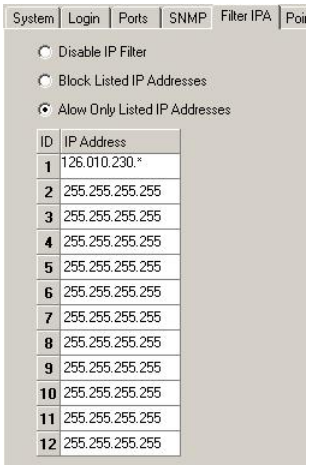


Fig. 9.1. *Filter IPA tab*

The **Filter IPA** tab (Figure 9.1) enables a security feature that allows you to block listed IP addresses, or allow traffic only from specific IP addresses. You can list up to 12 IP addresses in the Filter IPA list.

To block or allow all traffic from an IP subnet, you can type in an IP address in which an octet has been replaced with a **wild card character (*)**. For example, in Figure 9.1, Filter IPA has been configured to allow traffic only from the subnet **126.10.230.***.

The three radio buttons at the top of the tab give you three options:

Disable IP Filter: The default option, which disables all IP filtering.

Block Listed IP Addresses: Block all traffic from the listed IP addresses.

Allow Only Listed IP Addresses: Block traffic from all IP addresses **except** the listed IP addresses.

Any option selected acts on all IP addresses in the Filter IPA list. The Filter IPA settings apply to all inbound traffic over both the Public and Private Ethernet ports.

10 Point Groups Tab: Organize Alarms in Logical Categories

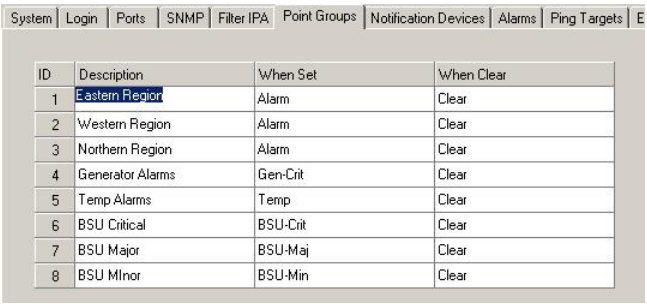


Fig. 10.1. *Point Groups tab*

The **Point Groups** tab provides a means of grouping alarm points and control relays into logical categories. You can use the Point Groups feature to organize alarms by severity or any other criteria you choose.

The NetGuardian-16S supports Point Groups. Point Groups 6, 7, and 8 are reserved for the preconfigured alarm groups **BSU Critical, BSU Major** and **BSU Minor**. When the NetGuardian-16S is in **Standalone Mode**, alarms assigned to these point groups will trigger on audiovisual alert on the NetGuardian-16S's integrated Building Status Unit. (When the NetGuardian is in **Standard Mode**, the CopperCom CopperController controls which alarms trigger an integrated BSU audiovisual alert. For more information on the integrated BSU, see the NetGuardian-16S User Manual.)

The **Point Groups** tab is used only for **defining** Point Groups. You assign individual alarm points, control relays and notification contacts to Point Groups using the **Notification Devices, Alarms, Ping Targets** and **Relays** tabs. (For information, see Section 11, "Notification Devices Tab: Configure Pager and Email Notifications"; Section 12, "Alarms Tab: Configure Discretes and System Alarms"; Section 13, "Ping Targets Tab"; and Section 15, "Relays Tab.")

Each Point Group is defined by three text boxes, which are shown in the columns in the **Point Groups** tab:

Description: Type in a general label for this Point Group. (Note that Point Groups 6, 7 and 8 are reserved for the preconfigured alarm groups **BSU Critical, BSU Major** and **BSU Minor**. This box has a 16 character limit.

When Set: Type in a text notice you want users to see when alarms from this Point Group are set. This text will appear in SNMP Traps and responses, pager and email alarm notifications, TTY text alarms, and in the Web Browser Interface (in the **State** column of the **Base Alarms** and **Ping Targets** pages). If this box is left blank, the generic label, "**Alarm**," will be displayed when alarms from this Point Group are set. This box has an 8 character limit.

When Clear: Type in a text notice you want users to see when alarms from this Point Group are cleared. his text will appear in SNMP Traps and responses, pager and email alarm notifications, TTY text alarms, and in the Web Browser Interface (in the **State** column of the **Base Alarms** and **Ping Targets** pages). If this box is left blank, the generic label, "**Clear**," will be displayed when alarms from this Point Group are clear. This box has an 8 character limit.

11 Notification Devices Tab: Configure Pager and Email Alarm Notifications

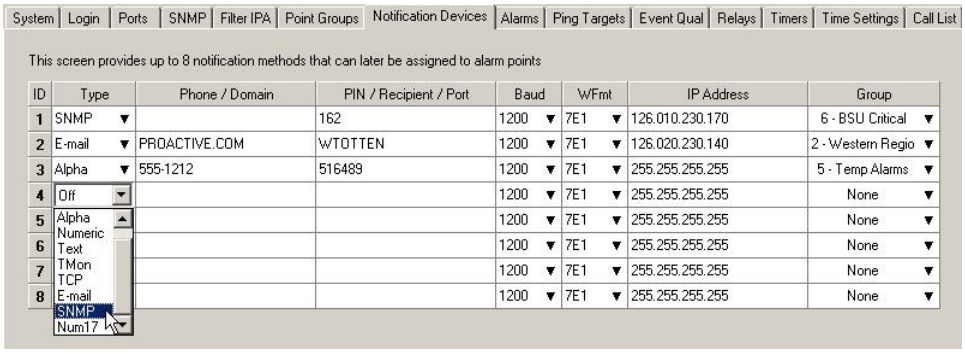


Fig. 11.1. *Notification Devices*

The **Notification Devices** tab (Figure 11.1) provides options for configuring the types of external notification devices used by the NetGuardian-16S. Up to eight notification devices can be defined, including additional SNMP Trap managers besides the primary and secondary SNMP Trap managers. You can configure multiple notification devices of the same type.

The **Notification Devices** tab is used only for **defining** what notification devices are available. You assign individual alarm points to notification devices using the **Alarms** and **Ping Targets** tabs. (For information, see Section 12, "Alarms Tab: Configure Discretes and System Alarms"; and Section 13, "Ping Targets Tab.")

For each notification device, there are several option fields to be defined. Please note that the option fields for each notification device will change to display the appropriate options for the device you select, and that some option fields are disabled for some device types.

Type	Description
Alpha	Alphanumeric paging that recognizes numbers, letters and symbols. Can display alarm point addresses, alarm descriptions, date/time stamps and alarm state.
Numeric	Numeric paging that recognizes only numbers. Message is reported in format [IP]*[Display][Address]*[State]. When displayed on pager, message appears in format ############ - #### - #.
Text	Text messages that can be accessed through terminal emulation software. Can display alarm point addresses, alarm descriptions, date/time stamps and alarm state.
TMon	Alarm forwarding to T/Mon NOC via dial-up connection. Can display alarm information, alarm description and threshold status.
Email	Email alarm notification. Can display alarm point addresses, alarm descriptions, date/time stamps and alarm state.
SNMP	Send SNMP Trap to tertiary SNMP Trap manager.
TCP	Alarm notification via TCP port. Connection from terminal must be established for TCP notification.
Num17	Numeric paging without * symbol. Message is reported in format [IP][Display][Address][State]. When displayed on pager, message appears in format ##################.

Table 11.A. *Notification Device types*

The following are the basic options for the **Notification Devices** tab. For detailed instructions for configuring each notification device type, see Sections 11.1–11.8.

Type: Choose from **Off, Alpha, Numeric, Text, TMon, TCP, E-mail, SNMP** or **Num17**. The Type options are explained in detail in Table 11.A, on page 19.

Phone/Domain: Type in a phone number (for pager notification) or an Internet domain (for email notification). The name in the field header will change to reflect the selected device type. This field is not required for some device types.

PIN/Recipient/Port: Type in a PIN (for alphanumeric pager notification), email recipient user name (for email notification) or port (for TCP and SNMP notification). The name in the field header will change to reflect the selected device type. This field is not required for some device types.

Baud: Choose a baud rate from the drop-down menu. This field is used only with **Alpha, Text** and **TMon**.

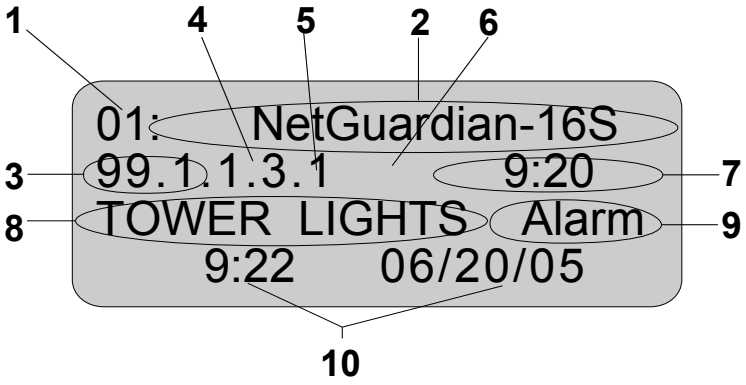
WFmt: Choose a word format from the drop-down menu. This field is used only with **Alpha, Text** and **TMon**.

IP Address: Type in an IP address for different network elements, depending on the selected notification device type. This field is used only with **E-mail, TCP** and **SNMP**.

Group: Choose a Point Group from the drop-down menu. This assigns all alarms from a Point Group to this notification device, so that, for example, all Critical alarms are sent to the

primary on-call technician, or all BSU Critical alarms are sent to an auxiliary SNMP Trap manager. (For information on defining Point Groups, see Section 10, "Point Groups Tab: Organize Alarms in Logical Categories." For information about assigning alarms to Point Groups, see Section 12, "Alarms Tab: Configure Discretes and System Alarms," and Section 13, "Ping Targets Tab.)

11.1 Alphanumeric Pager Setup



1. Number of pages
2. Unit name
3. Port # and Address (T/Mon NOC only)
4. Display number
5. Alarm point number
6. Alarm status: 1=alarm, 0=clear
7. Time NetGuardian-16 sent page
8. Alarm point description
9. Alarm status
10. Date and time pager received page

Fig. 11.1.1. *Typical alphanumeric pager alarm display*

If you select **Alpha** from the **Type** drop-down menu, the rest of your configuration options are:

Phone: Type in the pager's phone number.

PIN: Type in the pager's PIN (5–15 digits).

Baud: Choose from **1200, 2400** or **9600**. Default setting is 1200.

WFmt: Choose from **8N1, 7E1** or **7O1**. Default setting is 7E1.

Group: Choose a Point Group from the drop-down menu to assign all alarms from that group to this pager.

11.2 Numeric Pager Setup

If you select **Numeric** from the **Type** drop-down menu, the rest of your configuration options are:

Phone: Type in the pager's phone number, followed by commas. (For example, 555-1212,,,,,,,) Each comma after the phone number adds a 2 second pause, giving the pager time to answer before the NetGuardian-16S transmits the alarm information.

Group: Choose a Point Group from the drop-down menu to assign all alarms from that group to this pager.

11.3 Text Paging Setup

If you select **Text** from the **Type** drop-down menu, the rest of your configuration options are:

Phone: Type in the phone number of the text paging device.

Baud: Choose from **1200, 2400** or **9600**. Default setting is 1200.

WFmt: Choose from **8N1, 7E1** or **7O1**. Default setting is 7E1.

Group: Choose a Point Group from the drop-down menu to assign all alarms from that group to this device.

11.4 T/Mon NOC Notification Setup

f you select **TMon** from the **Type** drop-down menu, the rest of your configuration options are:

Phone: Type in the phone number of the T/Mon NOC.

Site Number: Type in the site number of the T/Mon NOC.

Baud: Choose from **1200, 2400** or **9600**. Default setting is 1200.

WFmt: Choose from **8N1, 7E1** or **7O1**. Default setting is 7E1.

Group: Choose a Point Group from the drop-down menu to assign all alarms from that group to T/Mon NOC.

11.5 E-Mail Setup

From: netguardian-16s@proactive.com
Sent: Wednesday, August 03, 2005 2:27 PM
To: wtotten@proactive.com
Subject: Event at Techlab.com

POINT 1 BULL PEN 2 ALARM

Fig. 11.5.1. *Typical email alarm notification*

If you select **E-mail** from the **Type** drop-down menu, the rest of your configuration options are:

Domain: Type in the Internet domain (everything after the @ sign) of the email recipient's email address.

Recipient: Type in the user name (everything before the @ sign) of the email recipient's email address.

IP Address: Type in the IP address of the SMTP server.

Group: Choose a Point Group from the drop-down menu to assign all alarms from that group to this email recipient.

11.5.1 Configuring the NetGuardian-16S's Display Email Address

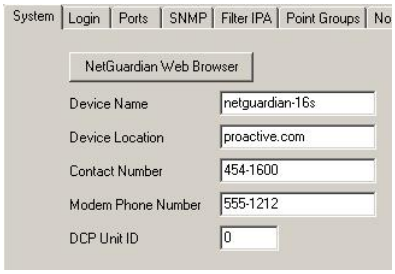


Fig. 11.5.1.1. *Assigning the NetGuardian-16S a display email address*

For identification purposes, it's a good idea to assign a display email address to the NetGuardian-16S. This doesn't have to be a real email address, but it will identify the NetGuardian-16S in the "From" line of all email alarm notifications sent from the unit.

To assign a display email address:

1. Click the **System** tab.
2. Enter the NetGuardian-16S's user name (everything in front of the @ sign) in the **Device Name** box.
3. Enter the NetGuardian-16S's Internet domain (everything after the @ sign) in the **Device Location** box.

11.5.2 Assigning a Password for SMTP POP3 Authentication

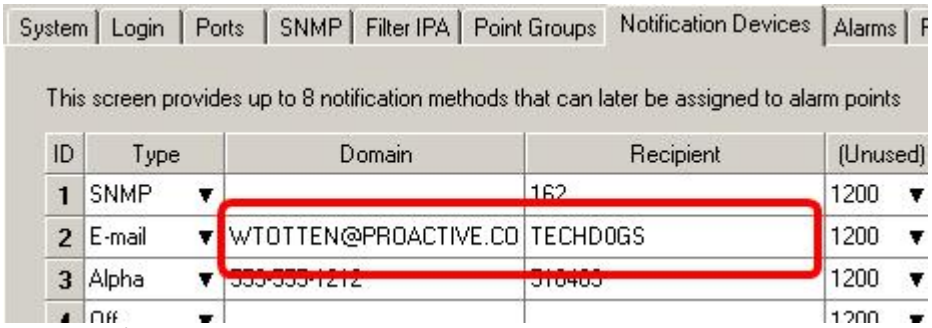


Fig. 11.5.2.1. *Configuring an SMTP authentication password*

Some SMTP servers require that email senders authenticate themselves with a password. You can configure the NetGuardian-16S to meet this requirement by authenticating itself with a password whenever it sends an email alarm notification.

To configure an SMTP authentication password:

1. Type in the email recipient's full email address in the **Domain** box (see Figure 11.5.2.1, above)
2. Type in the authentication password in the **Recipient** box.

11.6 SNMP Paging Setup

If you select **SNMP** from the **Type** drop-down menu, the rest of your configuration options are:

Port: Type in the UDP/IP port that the SNMP Trap manager receives Traps over. In most cases, this is Port 162.

IP Address: Type in the IP address of the SNMP Trap Manager.

Group: Choose a Point Group from the drop-down menu to assign all alarms from that group to this SNMP Trap Manager.

11.7 TCP Setup

<MSG_BEG 00001>
VID : DPS Telecom
FID : NetGuardian-16 v1.0B
SITE: Fresno
PNT : 99.01.01.01
DESC: RECTIFIER 1
STAT: CLEAR
DATE: 09/01/2005
TIME: 12:17:02
<MSG_END 00001>

Fig. 11.7.1. *An example TCP alarm notification*

Heading	Description
MSG_BEG MSG_END	Sequential message number used to group the message and detect missing messages (e.g. 00001, 00002, etc.).
VID	Vendor ID.
FID	NetGuardian-16S Firmware ID.
SITE	NetGuardian-16S system name.
PNT	Point ID (port.address.display.point). See Section 21.1, “Alarm Map”
DESC	Alarm description.
STAT	Status of the alarm (Clear or Alarm).
DATE	Date the alarm occurred.
TIME	Time the alarm occurred.

Table. 11.7.A. *TCP message elements*

The **TCP** notification device type transmits alarm notifications over the NetGuardian-16S's own TCP/IP port(s). To view a TCP alarm notification, a terminal must make a Telnet connection to the NetGuardian-16S's IP address's and the TCP/IP port defined on the **Notification Devices** tab. For example, if the NetGuardian-16S's IP address is 126.10.230.183 and TCP/IP Port 3000 is configured for TCP notification, you could monitor alarm notifications from the NetGuardian-16S by opening a terminal window and typing in the command **Telnet 126.10.230.183 3000**. This is a convenient way to quietly monitor the NetGuardian-16S from your PC desktop.

If you select **TCP** from the **Type** drop-down menu, the rest of your configuration options are:

Port: Type in the UDP/IP port that the SNMP Trap manager receives Traps over. In most cases, this is Port 162.

IP Address: Type in the IP address of the SNMP Trap Manager.

Group: Choose a Point Group from the drop-down menu to assign all alarms from that group to this SNMP Trap Manager.

11.8 Num17 Pager Setup

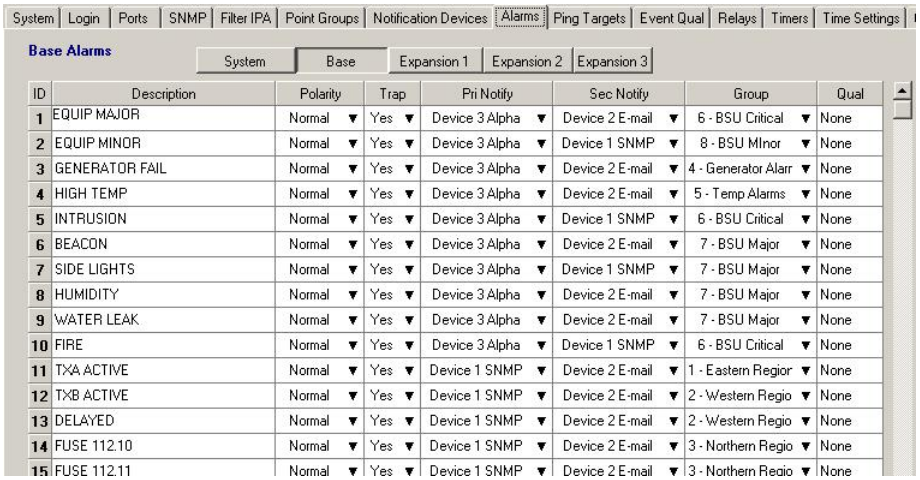
The **Num17** notification device type is much like the **Numeric** type, but Num17 eliminates the * symbol, which can cause problems on some pager systems.

If you select **Num17** from the **Type** drop-down menu, the rest of your configuration options are:

Phone: Type in the pager's phone number, followed by commas. (For example, 555-1212,,,,,,,) Each comma after the phone number adds a 2 second pause, giving the pager time to answer before the NetGuardian-16S transmits the alarm information.

Group: Choose a Point Group from the drop-down menu to assign all alarms from that group to this pager.

12 Alarms Tab: Configure Discretes and System Alarms



ID	Description	Polarity	Trap	Pri Notify	Sec Notify	Group	Qual
1	EQUIP MAJOR	Normal	Yes	Device 3 Alpha	Device 2 E-mail	6 - BSU Critical	None
2	EQUIP MINOR	Normal	Yes	Device 3 Alpha	Device 1 SNMP	8 - BSU MInor	None
3	GENERATOR FAIL	Normal	Yes	Device 3 Alpha	Device 2 E-mail	4 - Generator Alarr	None
4	HIGH TEMP	Normal	Yes	Device 3 Alpha	Device 2 E-mail	5 - Temp Alarms	None
5	INTRUSION	Normal	Yes	Device 3 Alpha	Device 1 SNMP	6 - BSU Critical	None
6	BEACON	Normal	Yes	Device 3 Alpha	Device 2 E-mail	7 - BSU Major	None
7	SIDE LIGHTS	Normal	Yes	Device 3 Alpha	Device 1 SNMP	7 - BSU Major	None
8	HUMIDITY	Normal	Yes	Device 3 Alpha	Device 2 E-mail	7 - BSU Major	None
9	WATER LEAK	Normal	Yes	Device 3 Alpha	Device 2 E-mail	7 - BSU Major	None
10	FIRE	Normal	Yes	Device 3 Alpha	Device 1 SNMP	6 - BSU Critical	None
11	TXA ACTIVE	Normal	Yes	Device 1 SNMP	Device 2 E-mail	1 - Eastern Regior	None
12	TXB ACTIVE	Normal	Yes	Device 1 SNMP	Device 2 E-mail	2 - Western Regio	None
13	DELAYED	Normal	Yes	Device 1 SNMP	Device 2 E-mail	2 - Western Regio	None
14	FUSE 112.10	Normal	Yes	Device 1 SNMP	Device 2 E-mail	3 - Northern Regio	None
15	FUSE 112.11	Normal	Yes	Device 1 SNMP	Device 2 E-mail	3 - Northern Regio	None

Fig. 12.1. *Configuring base alarms*

The **Alarms** tab (Figure 12.1) provides options for configuring the NetGuardian-16S's discrete alarm inputs.

At the top of the **Alarms** tab are two or more buttons: **System, Base** and (if NetGuardian Expansion units are connected to the NetGuardian-16S) **Expansion 1, Expansion 2** and **Expansion 3**. Clicking these buttons lets you view the NetGuardian-16S's system alarms, the discrete alarm inputs of the base NetGuardian-16S unit, and the discrete alarms of any NetGuardian Expansion units connected to the NetGuardian-16S.

Your choices, for each alarm point, are:

Description: Type a description of the alarm's function.

Polarity: Choose between **Normal** (normally open operation) and **Reversed** (normally closed operation).

Trap: Controls whether the NetGuardian-16S sends an SNMP Trap to the SNMP Trap manager(s) when this alarm is activated. Choose between **Yes** or **No**. Choosing Yes from this menu will send the alarm to both the primary and secondary SNMP Trap managers, if two Trap managers have been configured on the **SNMP** tab.

Pri Notify: To send this alarm to a notification device, choose the primary notification device from the drop-down menu.

Sec Notify: To send this alarm to a second notification device, choose the secondary notification device from the drop-down menu.

Group: To assign this alarm to a Point Group, choose the Point Group from the drop-down menu.

Qual: Double-click this box to configure qualification time for the alarm, the primary notification device, or the secondary notification device. For instructions on configuring event qualification times, see Section 12.1., "Configuring Event Qualification Timers."

12.1 Configuring Event Qualification Timers

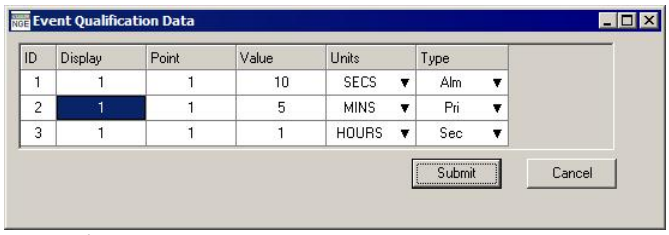


Fig. 12.1.1. *Event Qualification Data window*

Double-clicking in the **Qual** box for an alarm point opens the Event Qualification Data window (Figure 12.1.1, above). For each alarm point, you can set an alarm qualification time for:

1. **When the alarm is set**
2. **When the primary notification device is notified**
3. **When the secondary notification device is notified**

You can configure any of these notification times, or all three. There is a separate Event Qualification Data window for each alarm point, and three qualification events can be set for each alarm point. Your event qualification options are:

Display: ID number of the display of this alarm point. This setting cannot be edited.

Point: ID number this alarm point. This setting cannot be edited.

Value: Type in the number of time units for the qualification time.

Units: Choose the time units from the drop-down menu. Choose from seconds, minutes or hours.

Type: Choose the event to be qualified from the drop-down menu. Choose from **Ala** (time when alarm is declared set), **Pri** (time when primary notification device is notified) and **Sec** (time when secondary notification device is notified).

When you have made your choices, click **Submit** to save your settings or click **Cancel**.

12.2 System Alarms

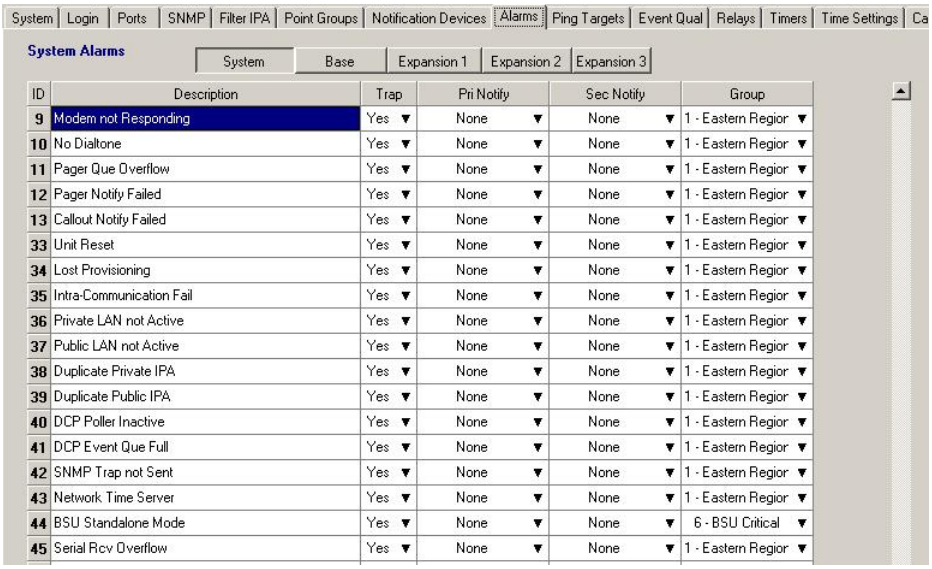

System
Login
Ports
SNMP
Filter IPA
Point Groups
Notification Devices
Alarms
Ping Targets
Event Qual
Relays
Timers
Time Settings
System Alarms
System
Base
Expansion 1
Expansion 2
Expansion 3
ID
Description
Trap
Pri Notify
Sec Notify
Group
9 Modem not Responding Yes None None 1 - Eastern Regior
10 No Dialtone Yes None None 1 - Eastern Regior
11 Pager Que Overflow Yes None None 1 - Eastern Regior
12 Pager Notify Failed Yes None None 1 - Eastern Regior
13 Callout Notify Failed Yes None None 1 - Eastern Regior
33 Unit Reset Yes None None 1 - Eastern Regior
34 Lost Provisioning Yes None None 1 - Eastern Regior
35 Intra-Communication Fail Yes None None 1 - Eastern Regior
36 Private LAN not Active Yes None None 1 - Eastern Regior
37 Public LAN not Active Yes None None 1 - Eastern Regior
38 Duplicate Private IPA Yes None None 1 - Eastern Regior
39 Duplicate Public IPA Yes None None 1 - Eastern Regior
40 DCP Poller Inactive Yes None None 1 - Eastern Regior
41 DCP Event Que Full Yes None None 1 - Eastern Regior
42 SNMP Trap not Sent Yes None None 1 - Eastern Regior
43 Network Time Server Yes None None 1 - Eastern Regior
44 BSU Standalone Mode Yes None None 6 - BSU Critical
45 Serial Rcv Overflow Yes None None 1 - Eastern Regior

Fig. 12.2.1. *System alarms*

Click the **System** button on the **Alarms** tab to configure options for the NetGuardian-16S's internal housekeeping alarms. For a full description of the NetGuardian-16S's system alarms, see Section 20.2, "System Alarm Descriptions," in the Reference section.

Your configuration options for the system alarms are:

Description: Description of the alarm's function. This setting cannot be edited.

Trap: Controls whether the NetGuardian-16S sends an SNMP Trap to the SNMP Trap manager(s) when this alarm is activated. Choose between **Yes** or **No**. Choosing Yes from this menu will send the alarm to both the primary and secondary SNMP Trap managers, if two Trap managers have been configured on the **SNMP** tab.

Pri Notify: To send this alarm to a notification device, choose the primary notification device from the drop-down menu.

Sec Notify: To send this alarm to a second notification device, choose the secondary notification device from the drop-down menu.

Group: To assign this alarm to a Point Group, choose the Point Group from the drop-down menu. Note that one system alarm, **BSU Standalone Mode** is preconfigured for Point Group 6, **BSU Critical.**

13 Ping Targets Tab: Configure Ping Alarms

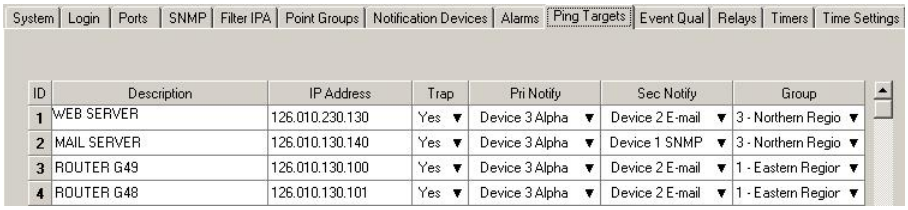


Fig. 13.1. *Configuring ping alarms*

The **Ping Targets** tab (Figure 13.1) provides options for configuring the NetGuardian-16S's 32 ping alarms. Your choices, for each ping target, are:

Description: Type a description of the device being pinged.

IP Address: Type in the IP address of the device being pinged.

Trap: Controls whether the NetGuardian-16S sends an SNMP Trap to the SNMP Trap manager(s) when this alarm is activated. Choose between **Yes** or **No**. Choosing Yes from this menu will send the alarm to both the primary and secondary SNMP Trap managers, if two Trap managers have been configured on the **SNMP** tab.

Pri Notify: To send this alarm to a notification device, choose the primary notification device from the drop-down menu.

Sec Notify: To send this alarm to a second notification device, choose the secondary notification device from the drop-down menu.

Group: To assign this alarm to a Point Group, choose the Point Group from the drop-down menu.

14 Event Qual Tab: View All Event Qualification Times

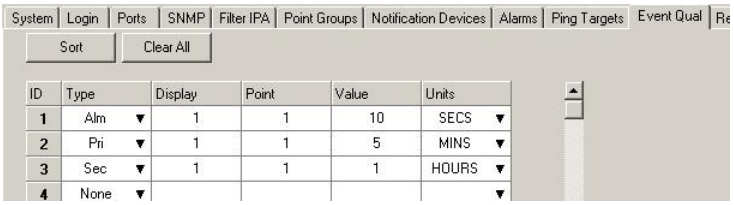


Fig. 14.1. *Event Qual tab*

The **Event Qual** tab (Figure 14.1) presents a bird's-eye view of all event qualification times for all alarm points. You can edit event qualification timers in this tab, although it's easier to keep track of what you're doing if you edit the qualification times on the **Alarms** tab.

At the top of the **Event Qual** tab are two buttons: **Sort** and **Clear**. Clicking the **Sort** button reorganizes the event qualification entries in ascending order of display and point.

Fig. 14.2. *Type in "yes" to confirm that you want to clear all event qualification times*

Clicking the **Clear** button will erase all event qualification times. Clicking this button will first open the confirmation dialog box shown in Figure 14.2, above. Type "yes" and click **Clear All** to erase all qualification times. Click **Don't Make Any Changes** to cancel the erasure and dismiss the dialog box.

For every entry in the Event Qualifier table, your options are:

Type: Choose the event to be qualified from the drop-down menu. Choose from **Ala** (time when alarm is declared set), **Pri** (time when primary notification device is notified) and **Sec** (time when secondary notification device is notified).

Display: ID number of the display of this alarm point.

Point: ID number of this alarm point. This setting cannot be edited.

Value: Type in the number of time units for the qualification time.

Units: Choose the time units from the drop-down menu. Choose from seconds, minutes or hours.

15 Relays Tab: Configure Control Relays

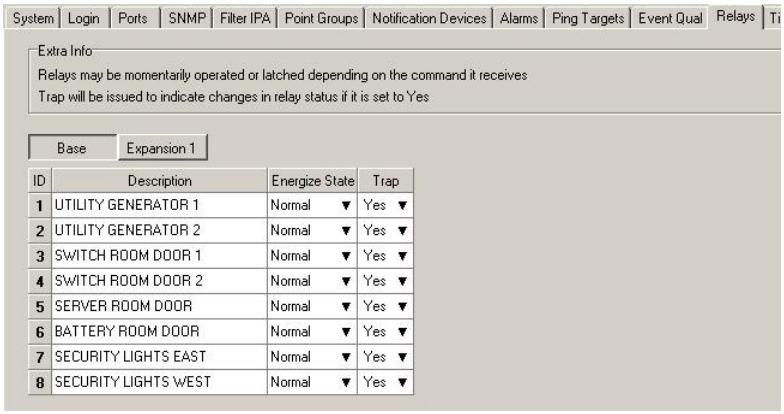


Fig. 15.1. *Relays tab*

The **Relays** tab (Figure 15.1) provides options for configuring the NetGuardian-16S's control relays.

At the top of the **Relays** tab are one or more buttons: **Base** and (if NetGuardian Expansion units are connected to the NetGuardian-16S) **Expansion 1, Expansion 2** and **Expansion 3**. Clicking these buttons lets you view the control relays of the NetGuardian-16S base unit, plus any NetGuardian Expansion units connected to the NetGuardian-16S.

Your choices, for each alarm point, are:

Description: Type a description of the control relay's function.

Polarity: Choose between **Normal** (normally open operation) and **Inverted** (normally closed operation).

Trap: Controls whether the NetGuardian-16S sends an SNMP Trap to the SNMP Trap manager(s) when this control relay is activated. Choose between **Yes** or **No**. Choosing Yes from this menu will send a Trap to both the primary and secondary SNMP Trap managers, if two Trap managers have been configured on the **SNMP** tab.

16 Timers Tab: Configure Ping Cycles, Timeouts and Refresh Rates

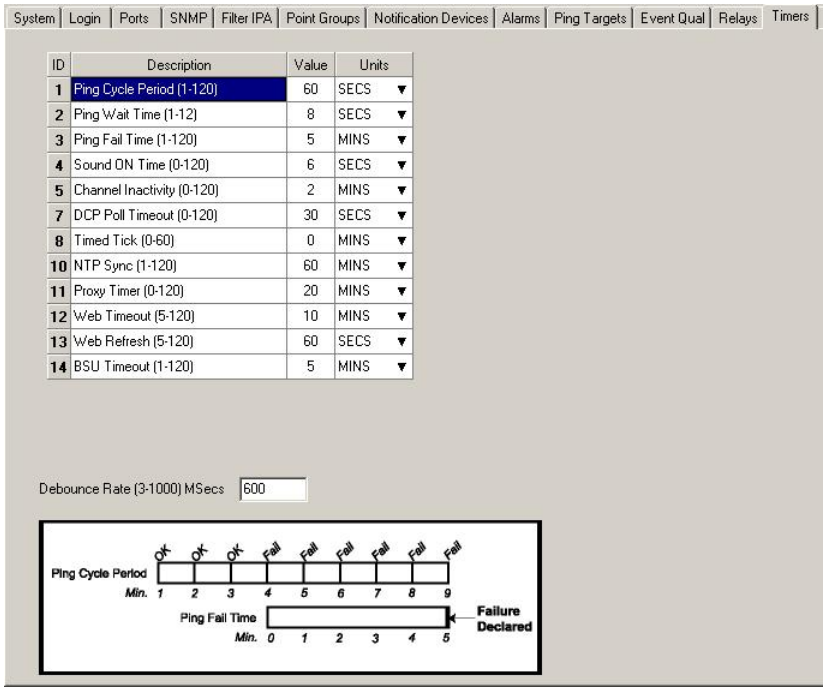


Fig 16.1. *Timers tab*

The **Timers** tab (Figure 16.1) provides options for configuring various time-related functions, such as ping cycles, timeout settings, refresh rates and so on. For each timer, the **Timers** tab lists the timer's:

Description: The function of the timer. (Timer functions are described in Section 16.1, "Timer Descriptions.") This box cannot be edited. This box also includes the acceptable range of values for this timer.

Value: Type in the number of time units for the qualification time.

Units: Choose the time units from the drop-down menu. Choose from seconds, minutes or hours. (Hours and minutes are not available for all timers.)

16.1 Timer Descriptions

Ping Cycle Period: How often the NetGuardian-16S pings each ping target. Range: 1–120 seconds. Default: 60 seconds. The smaller the Ping Cycle Period , the sooner you'll find out about network device failures — however, frequent pinging will increase your network traffic. The Ping Cycle Period should be set to several times the Ping Wait Time, to allow the ping target device time to respond.

Ping Wait Time: How long the NetGuardian-16S waits after sending a ping before it determines the target is unreachable. Range: 1–12 seconds. Default: 8 seconds.

Ping Fail Time: How long the NetGuardian-16S waits between an unsuccessful ping and determining that a ping target device has failed. Range: 1–120 minutes. Default: 5 minutes. The Ping Fail Time should be set to several times the Ping Cycle Period, to allow multiple pings before a device failure is declared.

Sound ON Time: How long the NetGuardian-16S's alarm speaker will sound when an alarm sets or clears. Range: 0–120 seconds. Default: 6 seconds. The alarm speaker can be manually turned off for one alarm at a time by pressing any front panel button. **Note:** This setting does not apply to audible alarms controlled by the NetGuardian-16S Integrated Building Status Unit.

Channel Inactivity: How long each data port may remain inactive before the port communication session is terminated. Range: 0–120 minutes. Default: 2 minutes. If the Channel Inactivity period elapses and the port session is terminated, the NetGuardian-16S will set System Alarm Point 47, Channel Port Timeout.

DCP Poll Timeout: How long the NetGuardian-16S waits after the last poll from a T/Mon master before determining that the T/Mon connection has failed. Range: 0–120 seconds. Default: 30 seconds. The DCP Poll timer is only active if DCP polling is enabled.

Timed Tick: How often the NetGuardian-16S toggles the state of System Alarm 46, Timed Tick. Range: 0–60 minutes. Default: 0 minutes. Timed Tick is a useful function for sending a heartbeat alarm to alarm masters that do not periodically poll RTUs.

NTP Sync: How often the NetGuardian-16S will synchronize its internal clock against a Network Time Protocol Server. Range: 0–120 seconds or minutes. Default: 60 minutes.

Proxy Timer: How long a proxy connection may remain inactive before the proxy session is terminated. Range: 0–120 minutes. Default: 20 minutes. (Data ports set to permanent TCP, or PTCP, never time out regardless of the Proxy Timer setting.) Setting the Proxy Timer to zero proxy sessions never time out. This is not recommended, because a broken connection can tie up the proxy port, requiring a reboot or manual port reset.

Web Timeout: How long a Web Browser Interface connection may remain inactive before the user is required to log on again. Range: 5–120 minutes. Default: 10 minutes.

Web Refresh: How often the NetGuardian-16S will automatically refresh Web Browser Interface pages. Range: 5–120 seconds. Default: 60 seconds.

BSU Timeout: How long the NetGuardian-16S will wait between multiple unsuccessful pings of the CopperCom CopperController (as defined by the Ping Cycle Period and the Ping Wait Time and entering Standalone Mode. Range: 1–120 minutes. Default: 5 minutes.

Debounce Rate: How long alarm sensor signal must be active before the NetGuardian-16S detects a discrete alarm. Range: 3–1000 msec. Default: 600 msec.

17 Time Settings Tab

Fig. 17.1. *Time Settings tab*

The **Time Settings** tab (Figure 17.1) lets you configure the NetGuardian-16S to automatically set its internal clock to a Network Time Protocol server.

To enable network time sync, enter the IP address and port of a network time server. (For a list of network time servers, click the Web link.) Select your time zone in the **Time Zone** drop-down menu, and check the **Observe DST** check box if you're currently observing daylight saving time.

18 Call List Tab: Configure Voice Call Out

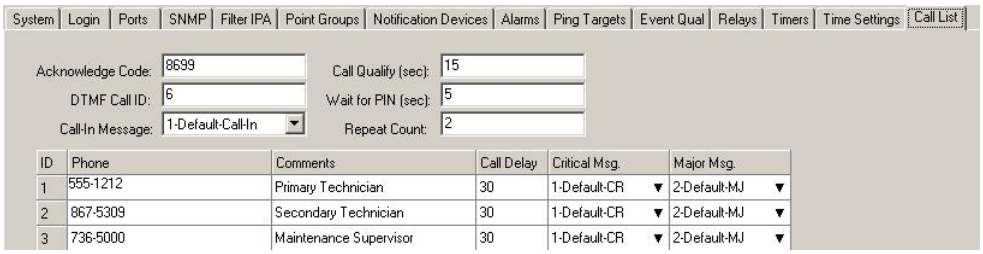


Fig. 18.1. *Call List tab*

The **Call List** tab (Figure 18.1) provides options for configuring the NetGuardian-16S Voice Call Out feature.

18.1 Global Voice Call Out Settings

The top portion of the **Call List** tab configures global Voice Call Out settings:

Acknowledge Code: DTMF code users enter to acknowledge alarms.

DTMF Call ID: ID number of pre-recorded voice message to be played at the start of the call to identify the NetGuardian-16S unit.

Call-In Message: Drop-down menu to select voice dialog for voice call-in. You have a choice of three default dialogs.

Call Qualify: Length of pause between Voice Call Out command issued by CopperController and initiation of dial out. Range: 5–99 sec. Default: 15 seconds.

Wait for PIN: Length of pause between message repetitions to allow user to enter Acknowledge Code. Range: 1–16 seconds. Default: 5 seconds

Repeat Count: Number of times NetGuardian-16S will repeat Voice Call Out dialog. If user does not enter Acknowledge Code within Repeat Count, the NetGuardian-16S will hang up and call next contact.

18.2 Contact-Specific Voice Call Out Settings

The lower portion of the **Call List** tab defines the list of Voice Call Out contacts. Up to 10 contacts can be defined. For each contact, your choices are:

Phone: Type in the contact's phone number.

Description: Optional description of the contact.

Call Delay: Incremental delay time from initial SNMP set or end of previous call before new call. Range: 0–00 seconds. Default: 30 seconds.

Critical Msg.: Drop-down menu to select voice dialog for Critical alarms. You have a choice of 16 dialogs. To turn off Critical notifications for this contact, choose **0-Don't Call**.

Major Msg.: Drop-down menu to select voice dialog for Major alarms. You have a choice of 16 dialogs. To turn off Major notifications for this contact, choose **0-Don't Call**.

18.3 Voice Call Out Sequence of Operations

1. In Standard Mode, Voice Call Out is initiated when the CopperCom CopperController sends an SNMP SET command. In Standalone Mode, Voice Call Out is initiated when an alarm occurs that has been assigned to Group 6 - BSU Critical or Group 7 - BSU Major by the system administrator.
2. If the modem is busy with data traffic, Voice Call Out is paused until the modem is clear.
3. If and when the modem is clear, Voice Call Out is paused for the Call Qual Time period set by the system administrator. (See Section 19, "Call List Tab" for configuration details.)
4. If the alarm that triggered Voice Call Out clears during the Call Qual Time, Voice Call Out will be canceled. (If the alarm clears during the call, Voice Call Out will play the message "Alarm Cleared" and hang up.)
5. Critical call outs always supersede Major call outs. If a Major call out is in progress when a Critical alarm occurs, the Major call out will be canceled. (If a Major call out is terminated during a call, the NetGuardian-16S will play the message "Critical abort" and hang up.)
6. When Voice Call Out is initiated, the NetGuardian-16S will dial the first number listed on the Call List for the alarm's severity level.
7. The NetGuardian-16S will play the dialog determined by the CopperController's SNMP SET command. If the SET command does not specify an alarm dialog, the NetGuardian-16S will play the dialog selected for this contact in the Call List.
8. The dialog will be repeated up as many times as specified in the Repeat Count setting (see Section 19, "Call List Tab," for configuration details). There will be a pause (controlled by Wait for PIN setting in the Call List Tab) after each repetition to allow the user to enter the DTMF acknowledge code.
9. The user can interrupt the dialog at any time by pressing the Star (*) key. The user can then enter the DTMF Acknowledge Code.
10. If the user makes a mistake entering the acknowledge code, he or she can clear the entry by pressing the Star (*) key.
11. If the user enters the correct code, the notification sequence will end.
12. If the call remains unacknowledged after a user-defined time period, the NetGuardian-16S will call the next contact listed in the Call List.
13. If the alarm clears during the call, the NetGuardian-16S will play the message "Alarm Cleared" and hang up. Critical clears will not cancel a Major call out, and Major clears will not cancel Critical call outs. Major call outs (but NOT Critical call outs) can also be aborted by pressing the BSU Ack button.
14. The notification sequence will continue until the alarm is acknowledged or the NetGuardian-16S has attempted to reach every contact on the Call List. A system alarm will be declared if no contact successfully acknowledged the alarm.

19 Voice Call Out Default Dialogs

19.1 Dialog 1: Default Critical

"Hello, this is telephone number <DTMF ID>."

"The time is <time> <A.M./P.M.>"

"A Critical alarm exists. A Critical alarm exists. A Critical alarm exists."

"Enter PIN to acknowledge alarm."

(User enters Acknowledge Code followed by pound (#) to acknowledge alarm.)

If **Wait for PIN** time elapses, and the user has not entered the code, then replay message.

If user enters incorrect code, then: **"Problem invalid acknowledgement code."**

If errors exceed repeat count, then: **"Thank you. Goodbye."**

If code correct then: **"Acknowledgement accepted. Thank you. Goodbye."**

19.2 Dialog 2: Default Major

"Hello, this is telephone number <DTMF ID>."

"The time is <time> <A.M./P.M.>"

"A Major alarm exists. A Major alarm exists. A Major alarm exists."

"Enter PIN to acknowledge alarm."

(User enters Acknowledge Code followed by pound (#) to acknowledge alarm.)

If **Wait for PIN** time elapses, and the user has not entered the code, then replay message.

If user enters incorrect code, then: **"Problem invalid acknowledgement code."**

If errors exceed repeat count, then: **"Thank you. Goodbye."**

If code correct then: **"Acknowledgement accepted. Thank you. Goodbye."**

19.3 Dialog 3: Default Secure Dial-In

"Please enter password."

(User enters Acknowledge Code followed by pound (#) as user ID password.)

"Hello, this is telephone number <DTMF ID>."

"The time is <time> <A.M./P.M.>"

If no alarms, then: **"No alarms exist. No alarms exist. No alarms exist."**

If Critical alarm, then: **"A Critical alarm exists. A Critical Alarm exists. A Critical Alarm exists."**

If Major alarm, then: **"A Major alarm exists. A Major Alarm exists. A Major Alarm exists."**

"Thank you. Goodbye."

19.4 Dialog 4: Critical GR-474

"Hello, this is telephone number <DTMF ID>."

"The time is <time> <A.M./P.M.>"

"A Critical alarm exists. A Critical alarm exists. A Critical alarm exists."

BONG-BONG, BONG-BONG, BONG-BONG *(Double-stroke "bong" every 1.5 seconds, 6 strokes total)*

"Enter PIN to acknowledge alarm."

(User enters Acknowledge Code followed by pound (#) to acknowledge alarm.)

If **Wait for PIN** time elapses, and the user has not entered the code, then replay message.

If user enters incorrect code, then: **"Problem invalid acknowledgement code."**

If errors exceed repeat count, then: **"Thank you. Goodbye."**

If code correct then: **"Acknowledgement accepted. Thank you. Goodbye."**

19.5 Dialog 5: Major GR-474

"Hello, this is telephone number <DTMF ID>."

"The time is <time> <A.M./P.M.>"

"A Major alarm exists. A Major alarm exists. A Major alarm exists."

BONG, BONG, BONG *(Single "bong" every 1.5 seconds, 3 strokes total)*

"Enter PIN to acknowledge alarm."

(User enters Acknowledge Code followed by pound (#) to acknowledge alarm.)

If **Wait for PIN** time elapses, and the user has not entered the code, then replay message.

If user enters incorrect code, then: **"Problem invalid acknowledgement code."**

If errors exceed repeat count, then: **"Thank you. Goodbye."**

If code correct then: **"Acknowledgement accepted. Thank you. Goodbye."**

19.6 Dialog 6: GR-474 Secure Dial-In

"Please enter password."

(User enters Acknowledge Code followed by pound (#) as user ID password.)

"Hello, this is telephone number <DTMF ID>."

"The time is <time> <A.M./P.M.>"

If no alarms, then: **"No alarms exist. No alarms exist. No alarms exist."**

If Critical alarm, then:

"A Critical alarm exists. A Critical Alarm exists. A Critical Alarm exists."

BONG-BONG, BONG-BONG, BONG-BONG *(Double-stroke "bong" every 1.5 seconds, 6 strokes total)*

If Major alarm, then:

"A Major alarm exists. A Major Alarm exists. A Major Alarm exists."

BONG, BONG, BONG *(Single "bong" every 1.5 seconds, 3 strokes total)*

"Thank you. Goodbye."

19.7 Dialog 7: Critical RUS-FORM-522

"Hello, this is telephone number <DTMF ID>."

"The time is <time> <A.M./P.M.>"

"A Critical alarm exists. A Critical alarm exists. A Critical alarm exists."

"Enter PIN to acknowledge alarm."

(User enters Acknowledge Code followed by pound (#) to acknowledge alarm.)

If **Wait for PIN** time elapses, and the user has not entered the code, then replay message.

If user enters incorrect code, then: **"Problem invalid acknowledgement code."**

If errors exceed repeat count, then: **"Thank you. Goodbye."**

If code correct then: **"Acknowledgement accepted. Thank you. Goodbye."**

19.8 Dialog 8: Major RUS-FORM-522

"Hello, this is telephone number <DTMF ID>."

"The time is <time> <A.M./P.M.>"

"A Major alarm exists. A Major alarm exists. A Major alarm exists."

BUSY-BUSY-BUSY *(Busy tone, 3 pulses; .5 seconds on and .5 seconds off)*

"Enter PIN to acknowledge alarm."

(User enters Acknowledge Code followed by pound (#) to acknowledge alarm.)

If **Wait for PIN** time elapses, and the user has not entered the code, then replay message.

If user enters incorrect code, then: **"Problem invalid acknowledgement code."**

If errors exceed repeat count, then: **"Thank you. Goodbye."**

If code correct then: **"Acknowledgement accepted. Thank you. Goodbye."**

19.9 Dialog 9: RUS-FORM-522 Secure Dial-In

"Please enter password."

(User enters Acknowledge Code followed by pound (#) as user ID password.)

"Hello, this is telephone number <DTMF ID>."

"The time is <time> <A.M./P.M.>"

If no alarms, then:

"No alarms exist. No alarms exist. No alarms exist."

RING-RING, RING-RING, RING-RING... (Continuous 2-ring ringback tone)

If Critical alarm, then:**"A Critical alarm exists. A Critical Alarm exists. A Critical Alarm exists."**

If Major alarm, then:

"A Major alarm exists. A Major Alarm exists. A Major Alarm exists."

BUSY-BUSY-BUSY *(Busy tone, 3 pulses; .5 seconds on and .5 seconds off)*

"Thank you. Goodbye."

20 Firmware Load

Your NetGuardian-16S ships with the latest firmware already loaded. But DPS Telecom periodically releases free firmware updates to add new improvements to its products. You can get the best of new features without having to replace your hardware. You're entitled to free firmware updates for the lifetime of your NetGuardian-16S unit.

To upload new firmware to your NetGuardian-16S unit(s), all you need is a LAN connection to the unit(s) and the Edit16S software. You can upload firmware to one NetGuardian-16S unit at a time or to multiple units.

For specific, step by step instructions for installing firmware updates, see the following sections:

- Section 19.1: "Loading Firmware on a Single NetGuardian-16S Unit"
- Section 19.2: "Loading Firmware on Multiple NetGuardian-16S Units Using Saved Configuration Files"
- Section 19.3 "Loading Firmware on Multiple NetGuardian-16S Units Using a Script File"

A note on firmware updates: The NetGuardian-16S has two processors, one on its top circuit board, the other on its bottom circuit board. Each processor requires its own firmware. You can update the top or the bottom boards separately or simultaneously. **It's impossible to load a firmware update on the wrong board** — Edit16S detects which processor a firmware update is designed for and will not load firmware to the wrong board.

Your NetGuardian-16S ships with the latest firmware already loaded. But DPS Telecom periodically releases free firmware updates to add new improvements to its products. You can get the best of new features without having to replace your hardware. You're entitled to free firmware updates for the lifetime of your NetGuardian-16S unit.

To upload new firmware to your NetGuardian-16S unit(s), all you need is a LAN connection to the unit(s) and the Edit16S software. You can upload firmware to one NetGuardian-16S unit at a time or to multiple units.

A note on firmware updates: The NetGuardian-16S has two processors, one on its top circuit board, the other on its bottom circuit board. Each processor requires its own firmware. You can update the top or the bottom boards separately or simultaneously. **It's impossible to load a firmware update on the wrong board** — Edit16S detects which processor a firmware update is designed for and will not load firmware to the wrong board.

20.1 Loading Firmware on a Single NetGuardian-16S Unit

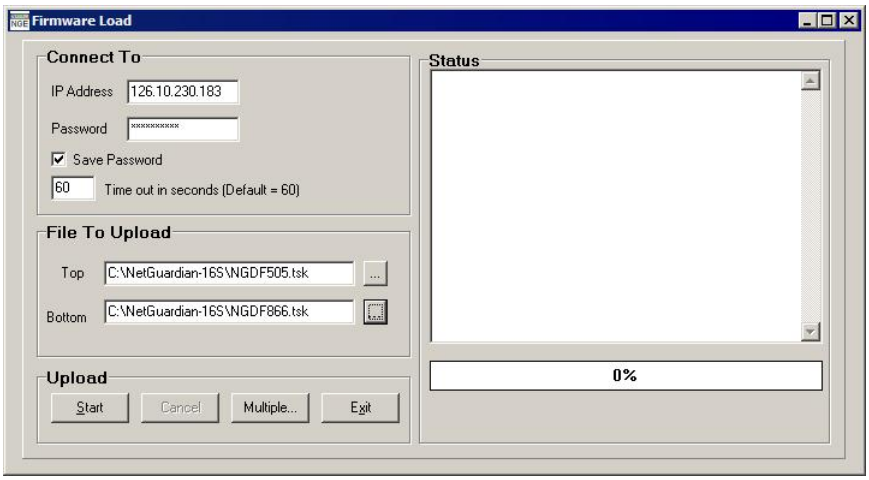


Fig. 20.1. *Firmware Load window*

To load new firmware on **one single NetGuardian-16S unit,** follow these steps:

1. Start Edit16S.
2. Choose **Load Firmware** from the **Device** menu, or click the **Load Firmware** button on the toolbar. **Note: The Load Firmware command is not available when a configuration file is open. You must close all configuration files to load firmware.**
3. Type in the IP Address and Password for the NetGuardian-16S unit you want to update. Checking the **Save Password** box will save your password and automatically prefill the Password box the next time you open the Load Firmware utility. Omit this step if you want to upload firmware to multiple NetGuardian-16S units.
4. The **Time out in seconds** box controls how long a Load Firmware connection can remain idle before it terminates. The default setting is 60 seconds.
5. In the **File To Upload** area, click the **Browse (...)** button for the circuit board you want to update. An Open dialog box will appear. Browse to the *.tsk file that contains the firmware update and click **Open.** You can update the Top and Bottom circuit boards separately or simultaneously. Edit16S will not load a firmware update on to the wrong board.
6. Click Start to upload firmware to one NetGuardian-16S. (To upload firmware to multiple units, click Multiple...)
7. The progress of the firmware load will be displayed in the **Status** pane. When the upload is complete, the NetGuardian-16S will automatically reboot.

20.2 Loading Firmware to Multiple NetGuardian-16S Units Using Saved Configuration Files (The Easy Way)

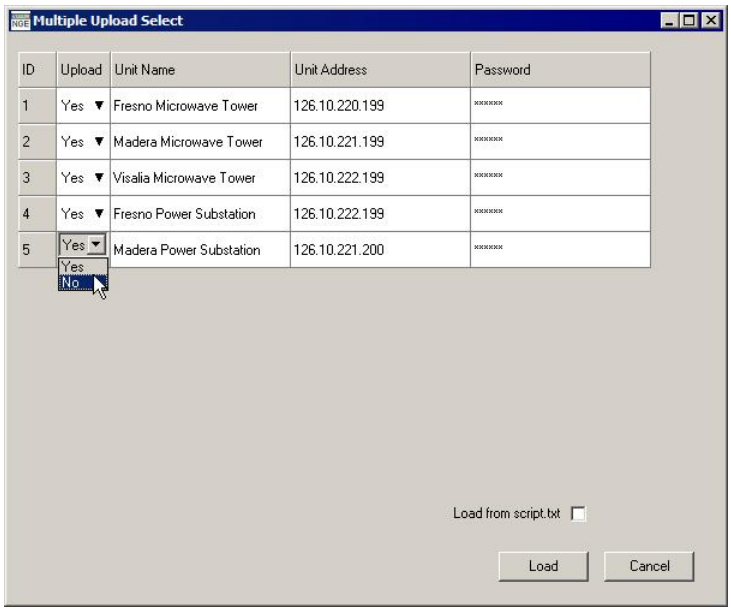


Fig. 20.2. *Multiple Upload Select window*

To upload firmware to multiple NetGuardian-16S units, Edit16S needs a list of the units to update and their IP addresses. The simple way to update multiple units is to point Edit16S to the list it already has — the saved configuration files on your PC's hard drive.

(For instructions on working with Edit16S configuration files, see Section 4.3, "Reading and Writing Configuration Files on PC Disk," and Section 4.4, "Reading and Writing Configuration Files to NetGuardian-16S NVRAM.")

To load new firmware to multiple NetGuardian-16S units using saved configuration files, follow these steps:

1. Start Edit16S.
2. Choose **Load Firmware** from the **Device** menu, or click the **Load Firmware** button on the toolbar. **Note: The Load Firmware command is not available when a configuration file is open. You must close all configuration files to load firmware.**
3. Click the **Multiple...** button.
4. The **Multiple Upload Select** window will open (see Figure 19.2.1). This window will list all the NetGuardian-16S devices for which you have Edit16S configuration files saved on your PC. **You must have a Edit16S configuration file for every NetGuardian-16S unit you want to update.**
5. By default, all units will be selected for upload. To unselect a unit, choose **No** from the **Upload** drop-down menu.
6. Do **not** check the **Load from script.txt** checkbox. For instructions on using this feature, see Section 19.3, "Loading Firmware to Multiple NetGuardian-16S Units Using a Script File."
7. After you've made sure the correct NetGuardian-16S units are selected, click the **Load** button. The multiple upload will proceed automatically. The Multiple Upload Select window will close. The **Status** pane in the main **Load Firmware** window will display the progress of the upload. Each NetGuardian-16

unit being updated will reboot automatically when its firmware load is complete.

20.3 Loading Firmware to Multiple NetGuardian-16S Units Using a Script File

The alternative way to update firmware on multiple firmware is to supply Edit16S with a script file. This is a plain text file that lists the firmware updates to install, the NetGuardian-16S units to update, and the IP address of each unit. **The script file must be titled "script.txt" and it must be placed in the same directory as the Edit16S executable file** — typically C:\Program Files\DPS Telecom\Edit16S\.
Here is a sample script file:

```
;     Script File.
;
; In order for this script to work properly please follow
the following rules:
;
;  1. Everything after semicolon is a comment.
;  2. Blank lines are allowed.
;  3. Retry, Delay, Password, and SourceFile values can be
reset.
;     New Values would apply to all IPAs that follow.
;  4. "Retry=X" will set number of retries to value X.
;  5. "Delay=X" will set delay value to X minutes.
;  6. "Password=samplepassword" will set password to
"samplepassword"
;  7. "SourceFile=C:\Directory\filename.tsk" will reset
source file.
;  8. Lines that are not flagged Comment, Retry, Delay,
Password or
;     SourceFile are read as IP addresses.

 Retry=1 ;Retry
 Delay=1 ;Retry Delay

;  Update NetGuardian-16S units in North Region
 Password=northrtus
;  Update bottom circuit boards
 SourceFile=C:\NetGuardian-16S\NGDF505.tsk
 126.10.230.183
 126.10.230.193
 126.10.230.203
;  Update top circuit boards
 SourceFile=C:\NetGuardian-16S\NGDF948.tsk
 126.10.230.183
 126.10.230.193
 126.10.230.203

;  Update NetGuardian-16S units in SouthRegion
 Password=sourthrtus
;  Update bottom circuit boards
 SourceFile=C:\NetGuardian-16S\NGDF505.tsk
 126.10.230.213
 126.10.230.223
 126.10.230.233
;  Update top circuit boards
 SourceFile=C:\NetGuardian-16S\NGDF948.tsk
 126.10.230.213
 126.10.230.223
 126.10.230.233
```

Fig. 20.3 *Sample script file*

Editing the Script File
The sample script file provided contains instructions for editing the file.
Updating Firmware Using the Script File
To use the script file to load new firmware on multiple NetGuardian-16S units, follow these steps:

1. Start Edit16S.
2. Choose **Load Firmware** from the **Device** menu, or click the **Load Firmware** button on the toolbar. **Note: The Load Firmware command is not available when a configuration file is open. You must close all configuration files to load firmware**.
3. Click the **Multiple...** button.
4. The **Multiple Upload Select** window will open.
5. Check the **Load from script.txt** checkbox. Edit16S will load the script file. **The script file must be titled "script.txt" and it must be placed in the same directory as the Edit16S executable file** — typically C:\Program Files\DPS Telecom\Edit16S\.
6. Click the **Load** button. The multiple upload will proceed automatically. The Multiple Upload Select window will close. The **Status** pane in the main **Load Firmware** window will display the progress of the upload. Each NetGuardian-16 unit being updated will reboot automatically when its firmware load is complete.

21 Reference Section

21.1 NetGuardian-16S Alarm Map

Description	Port	Address	Display	Points	SNMP Trap Numbers	
					Set	Clear
NetGuardian-16S Base Unit						
Discrete Alarms	99	1	1	1–32	8001–8032	9001–9032
Ping Alarms	99	1	2	1–32	8065–8096	8065–9096
Control Relays	99	1	11	1–8	8641–8648	9641–9648
System Alarms 9–15	99	1	11	9–15	8649–8655	9649–9655
System Alarms 33–50	99	1	11	33–50	8673–8690	9673–9690
NetGuardian Expansion #1						
Discrete Alarms	99	1	12	1–48	6001–6064	7001–7064
Control Relays	99	1	13	1–8	6065–6072	7065–7072
NetGuardian Expansion #2						
Discrete Alarms	99	1	14	1–48	6129–6177	7129–7177
Control Relays	99	1	15	1–8	6193–6200	7193–7200
NetGuardian Expansion #3						
Discrete Alarms	99	1	16	1–48	6257–6305	7257–7305
Control Relays	99	1	17	1–8	6321–6328	7321–7328

Table 20.1.A. *NetGuardian-16S alarm map*

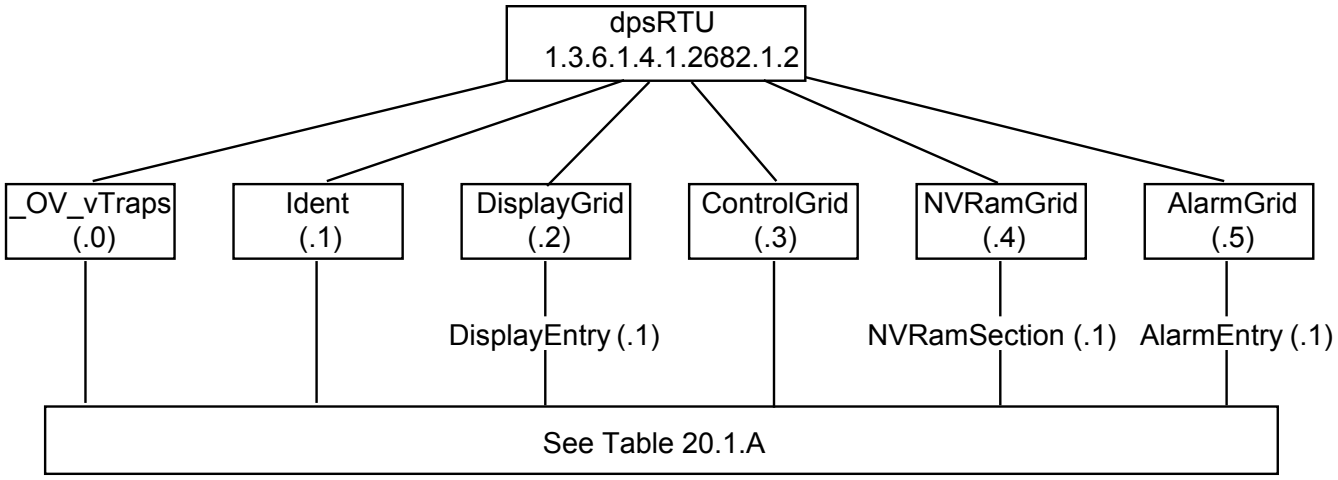
21.2 System Alarm Descriptions

Point	System Alarm	Description
9	Modem not Responding	Modem not responding to initialization string
10	No Dialtone	Dial tone not detected during dial-out attempt
11	Pager Que Overflow	Over 250 unsent events in pager queue
12	Pager Notify Failed	Attempted pager notification unsuccessful
13	Callout Que Overflow	Over 8 unsent calls in Voice Call Out queue
14	Callout Notify Failed	Attempted Voice Call Out unsuccessful
15	Exp. Module Callout	Alarm collected from Entry Control Unit (ECU)
33	Unit Reset	Toggles whenever unit reboots
34	Lost Provisioning	Unit using default configuration settings. NVRAM may be damaged
35	Intra-communication Fail	Communications failure between the NetGuardian-16S's two circuit boards
36	Private LAN not Active	Ethernet link not detected on Private port
37	Public LAN not Active	Ethernet link not detected on Public port
38	Duplicate Private IPA	Unit detects another node with same IP address as the Private port
39	Duplicate Public IPA	Unit detects another node with same IP address as the Public port
40	DCP Poller Inactive	Unit has not received poll from T/Mon for longer than DCP Timer period set by system administrator
41	DCP Event Que Full	More than 500 uncollected events in DCP event queue
42	SNMP Trap not Sent	SNMP trap address is not defined and an SNMP Trap event occurred
43	Network Time Server	Communication to network time server failure
44	BSU Standalone Mode	Communication with CopperController failure and BSU enters Standalone Mode.
45	Serial Rcv Overflow	UART hardware overflowed during receive
46	Serial Rcv Que Full	Alarm set when any data port is filled with more than 16K of information
47	Timed Tick	Toggles state at constant rate set by Timed Tick period configured by system administrator
48	Channel Port Timeout	Channel port has not forwarded any traffic for longer than Channel Port Timeout period set by system administrator
49	Craft Port Timeout	Craft Timeout Timer has not been reset in the period set by system administrator
50	NGDdx Expansion Fail	Communication to NetGuardian Expansion unit(s) failure

Table 20.2.A. *System alarm descriptions*

21.3 NetGuardian-16S Trap OIDs

The illustration and tables below outline the SNMP OIDs for NetGuardian-16S alarm points. This illustration begins with dpsRTU; however, the MIB object identifier tree has several levels above that. The full English name is as follows: root.iso.org.dod.internet.private.enterprises.dps-Inc.dpsAlarmControl.dpsRTU. Therefore, dpsRTU's full object identifier is 1.3.6.1.4.1.2682.1.2. Each level beyond dpsRTU adds another object identifying number. For example, the object identifier of the Display portion of the Control Grid is 1.3.6.1.4.1.2682.1.2.3.3 because the object identifier of dpsRTU is 1.3.6.1.4.1.2682.1.2 + the Control Grid (.3) + the Display (.3).



(O.)_OV_Traps points
_OV_vTraps (1.3.6.1.4.1.2682.1.2.0)
PointSet (.20)
PointClr (.21)
SumPSet (.101)
SumPClr (.102)
ComFailed (.103)
ComRestored (.014)
P0001Clr (.20001) through P0064Set (.10064)
P0001Clr (.20001) through P0064Clr (.20064)

(.1) Identity points
Ident (1.3.6.1.4.1.2682.1.2.1)
Manufacturer (.1)
Model (.2)
Firmware Version (.3)
DateTime (.4)
ResyncReq (.5)*
* Must be set to "1" to perform the resync request which will resend TRAPs for any standing alarm.

(.2) DisplayGrid points
DisplayEntry (1.3.6.1.4.1.2682.1.2.2.1)
Port (.1)
Address (.2)
Display (.3)
DispDesc (.4)*
PntMap (.5)*

(.3) ControlGrid points
ControlGrid (1.3.6.1.4.1.2682.1.2.3)
Port (.1)
Address (.2)
Display (.3)
Point (.4)
Action (.5)

(.4) NVRamSection points
NVRamSection (1.3.6.1.4.2682.1.2.4.1)
NVsNmbr (.1)
NvsData (.2)
NvsStatus (.3)

(.5) AlarmEntry points
AlarmEntry (1.3.6.4.1.2682.1.2.5.1)
Aport (.1)
AAddress (.2)
ADisplay (.3)
APoint (.4)
APntDesc (.5)*
AState (.6)
* For specific alarm points, see Table 20.1.A.

Table 20.3.A. *MIB object identifier tree descriptions*

21.4 SNMP Granular Trap Packets

SNMP Header	Description
0	Version
Public	Request
Trap	Request
1.3.6.1.4.1.2682.1.2	Enterprise
126.10.230.181	Agent address
Enterprise Specific	Generic Trap
8001	Specific Trap
617077	Time stamp
1.3.7.1.2.1.1.1.0	Object
NetGuardian16S	Value
1.3.6.1.2.1.1.6.0	Object
1-800-622-3314	Value
1.3.6.1.4.1.2682.1.2.4.1.0	Object
01-02-1995 05:08:27.760	Value
1.3.6.1.4.1.2682.1.2.5.1.1.99.1.1.1	Object
99	Value
1.3.6.1.4.1.2682.1.2.5.1.2.99.1.1.1	Object
1	Value
1.3.6.1.4.1.2682.1.2.5.1.3.99.1.1.1	Object
1	Value
1.3.6.1.4.1.2682.1.2.5.1.4.99.1.1.1	Object
1	Value
1.3.6.1.4.1.2682.1.2.5.1.5.99.1.1.1	Object
Rectifier Failure	Value
1.3.6.1.4.1.2682.1.2.5.1.6.99.1.1.1	Object
Alarm	Value

Table 20.4.A. *Example of SNMP headers and descriptions*

Table 20.4.A shows the information contained in the SNMP Trap packets sent by the NetGuardian-16S. The NetGuardian-16S sends a unique, granular Trap OID for each alarm point, and the Trap includes the user-configured alarm description in a variable binding value field.

There are two ways your SNMP manager can identify alarms from the NetGuardian-16S:

- Read the unique, granular Traps OID for each alarm
- Read the generic Trap OID for any NetGuardian-16S Trap (1.3.6.1.4.1.2682.1.2.5.1.2.99.1.1.1) and parse the variable binding for the alarm description.

22 Technical Support

DPS Telecom products are backed by our expert Technical Support representatives, live human beings with the training and skills to solve your problems fast. To help us help you better, please take the following steps before calling Technical Support:

1. **Check the DPS Telecom Web site.**
   You will find answers to many common questions on the DPS Telecom Web site, at **www.dpstelecom.com/support**. Look here first for a fast solution to your problem.

2. **Prepare relevant information.**
   Having the important information about your DPS Telecom product ready to hand will help us answer your questions faster. Please have ready your hardware serial number and user number when you call. It's also handy to write down all other important information about your DPS Telecom product. But if you don't have all the information when you call, our Technical Support representatives can help you find it.

3. **Have access to troubled equipment.**
   Please be at or near your equipment when you call DPS Telecom Technical Support. This will help us solve your problem more efficiently.

4. **Call during Customer Support hours.**
   Customer support hours are Monday through Friday, from 7 A.M. to 6 P.M., Pacific time. During these hours Technical Support representatives are on duty in our fully equipped simulation lab.

DPS Technical Support Phone Number: **(559) 454-1600**

Emergency Assistance: *Emergency assistance is available 24 hours a day, 7 days a week. For emergency assistance after hours, allow the phone to ring until it is answered with a paging message. You will be asked to enter your phone number. An on-call technical support representative will return your call as soon as possible.*

Warranty

DPS Telecom warrants, to the original purchaser only, that its products a) substantially conform to DPS' published specifications and b) are substantially free from defects in material and workmanship. This warranty expires two years from the date of product delivery with respect to hardware and ninety days from the date of product delivery with respect to software. If the purchaser discovers within these periods a failure of the product to substantially conform to the specifications or that the product is not substantially free from defects in material and workmanship, the purchaser must promply notify DPS. Within reasonable time after notification, DPS will endeavor to correct any substantial non-conformance with the specifications or substantial defects in material and workmanship, with new or used replacement parts. All warranty service will be performed at the company's office in Fresno, California, at no charge to the purchaser, other than the cost of shipping to and from DPS, which shall be the responsiblity of the purchaser. If DPS is unable to repair the product to conform to the warranty, DPS will provide at its option one of the following: a replacement product or a refund of the purchase price for the non-conforming product. These remedies are the purchaser's only remedies for breach of warranty. Prior to initial use the purchaser shall have determined the suitability of the product for its intended use. DPS does not warrant a) any product, components or parts not manufactured by DPS, b) defects caused by the purchaser's failure to provide a suitable installation environment for the product, c) damage caused by use of the product for purposes other than those for which it was designed, d) damage caused by disasters such as fire, flood, wind or lightning unless and to the extent that the product specification provides for resistance to a defined disaster, e) damage caused by unauthorized attachments or modifications, f) damage during shipment from the purchaser to DPS, or g) any abuse or misuse by the purchaser.

THE FOREGOING WARRANTIES ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In no event will DPS be liable for any special, incidental, or consequential damages based on breach of warranty, breach of contract, negligence, strict tort, or any other legal theory. Damages that DPS will not be responsible for include but are not limited to, loss of profits; loss of savings or revenue; loss of use of the product or any associated equipment; cost of capital; cost of any substitute equipment, facilities or services; downtime; claims of third parties including customers; and injury to property.

For an additional fee DPS may, at its option, make available by written agreement only an extended warranty providing an additional period of time for the applicability of the standard warranty.

Technical Support

If a purchaser believes that a product is not operating in substantial conformance with DPS' published specifications or there appear to be defects in material and workmanship, the purchaser should contact our technical support representatives. If the problem cannot be corrected over the telephone and the product and problem are covered by the warranty, the technical support representative will authorize the return of the product for service and provide shipping information. If the product is out of warranty, repair charges will be quoted. All non-warranty repairs receive a 90-day warranty.

Free Tech Support is Only a Click Away

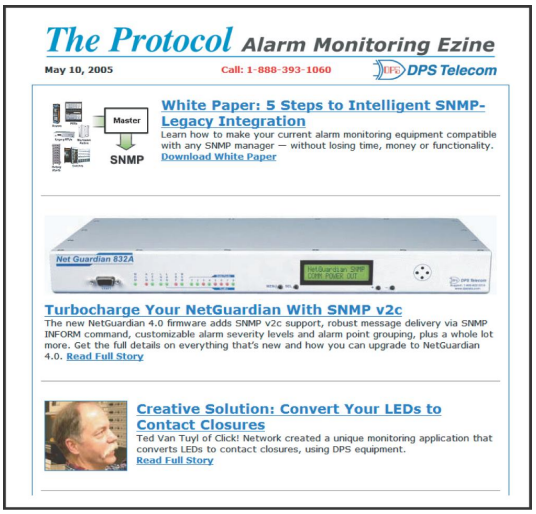
Need help with your alarm monitoring? DPS Information Services are ready to serve you … in your email or over the Web!

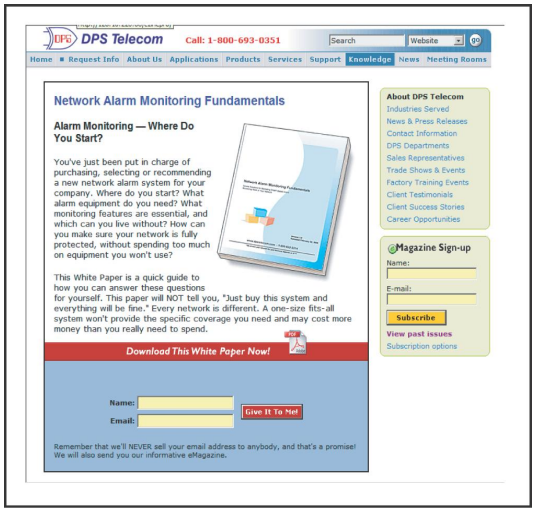
www.DpsTelecom.com

Free Tech Support in Your Email: The Protocol Alarm Monitoring Ezine

The Protocol Alarm Monitoring Ezine is your free email tech support alert, delivered directly to your in-box every two weeks. Every issue has news you can use right away:

- Expert tips on using your alarm monitoring equipment — advanced techniques that will save you hours of work
- Educational White Papers deliver fast informal tutorials on SNMP, ASCII processing, TL1 and other alarm monitoring technologies
- New product and upgrade announcements keep you up to date with the latest technology
- Exclusive access to special offers for DPS Telecom Factory Training, product upgrade offers and discounts


The Protocol Alarm Monitoring Ezine
May 10, 2005
Call: 1-888-393-1060
DPS Telecom
White Paper: 5 Steps to Intelligent SNMP-Legacy Integration
Learn how to make your current alarm monitoring equipment compatible with any SNMP manager — without losing time, money or functionality.
Download White Paper
Master
SNMP
Net Guardian 832A
Turbocharge Your NetGuardian With SNMP v2c
The new NetGuardian 4.0 firmware adds SNMP v2c support, robust message delivery via SNMP INFORM command, customizable alarm severity levels and alarm point grouping, plus a whole lot more. Get the full details on everything that's new and how you can upgrade to NetGuardian 4.0. Read Full Story
Creative Solution: Convert Your LEDs to Contact Closures
Ted Van Tuyl of Click! Network created a unique monitoring application that converts LEDs to contact closures, using DPS equipment.
Read Full Story


DPS Telecom
Call: 1-800-693-0351
Network Alarm Monitoring Fundamentals
Alarm Monitoring — Where Do You Start?
You've just been put in charge of purchasing, selecting or recommending a new network alarm system for your company. Where do you start? What alarm equipment do you need? What monitoring features are essential, and which can you live without? How can you make sure your network is fully protected, without spending too much on equipment you won't use?
This White Paper is a quick guide to how you can answer these questions for yourself. This paper will NOT tell you, "Just buy this system and everything will be fine." Every network is different. A one-size fits-all system won't provide the specific coverage you need and may cost more money than you really need to spend.
Download This White Paper Now!
Name:
Email:
Give It To Me!
Remember that we'll NEVER sell your email address to anybody, and that's a promise! We will also send you our informative eMagazine.
About DPS Telecom
Magazine Sign-up
Subscribe
View past issues

To get your free subscription to The Protocol register online at
www.TheProtocol.com/register

Free Tech Support on the Web: MyDPS

MyDPS is your personalized, members-only online resource. Registering for MyDPS is fast, free, and gives you exclusive access to:

- Firmware and software downloads and upgrades
- Product manuals
- Product datasheets
- Exclusive user forms

DPS Telecom
"Your Partners in Network Alarm Monitoring"

Register for MyDPS online at
www.DpsTelecom.com/register

(800) 622-3314 • www.DpsTelecom.com • 4955 E. Yale Avenue, Fresno, California 93727